华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- 1、华为E-learning 课程学习
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的“华为账号”和注册账号的“email地址”到 *Learning@huawei.com 申请权限。*
- 2、华为培训教材下载
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训->面授培训*”，在具体课程页面即可下载教材。
- 3、华为在线公开课(LVC)优先参与
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- 4、学习工具 eNSP
  - *eNSP (Enterprise Network Simulation Platform)*, 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，**与其他考生分享考试经验，一起学习华为产品技术。** （http://support.huawei.com/ecommunity/bbs/list_2247.html）



华为认证系列教程

HCNA-HNTD进阶
华为网络技术与设备



华为技术有限公司

版权声明

华为认证系列教程

HCNA-HNTD华为网络技术与设备

第2.0版本

华为认证体系介绍

依托华为公司雄厚的技术实力和专业的培训体系，华为认证考虑到不同客户对ICT技术不同层次的需求，致力于为客户提供实战性、专业化的技术认证。

根据ICT技术的特点和客户不同层次的需求，华为认证为客户提供面向十二个方向的三级认证体系。

HCNA主要面向IP网络维护工程师，以及其他希望学习IP网络知识的人士。HCNA认证在内容上涵盖TCP/IP基础、路由、交换等IP网络通用基础知识以及华为数据通信产品、通用路由平台VRP特点和基本维护。

HCNP-R&S主要面向企业级网络维护工程师、网络设计工程师以及希望系统深入地掌握路由、交换、网络调整及优化技术的人士。HCNP-R&S包括IESN（Implementing Enterprise Switching Networks，部署企业级交换网络）、IERN（Implementing Enterprise Routing Networks，部署企业级路由网络）、IENP（Improving Enterprise Network Performance，提升企业级网络性能）三个部分。内容上涵盖IPv4路由技术原理深入以及在VRP中的实现；交换技术原理深入以及在VRP中的实现；网络安全技术、高可靠性技术和Qos技术等高级IP网络技术以及在华为产品中的实现。

HCIE-R&S旨在培养能够熟练掌握各种IP网络技术，精通华为产品的维护、诊断和故障排除；具备大型IP网络规划、设计和优化的IP网络大师。

华为认证协助您打开行业之窗，开启改变之门，屹立在ICT世界的潮头浪尖！

建议进阶关系　必备进阶关系

ICT

	路由交换		无线局域网	无线	传送网	安全	统一通信		视讯	云计算	存储	ICT融合设计
工程师级	HCNA(HCDA)											
工程师级			HCNA-WLAN	HCNA-LTE	HCNA-Transmission	HCNA-Security	HCNA-UC	HCNA-CC	HCNA-VC	HCNA-Cloud	HCNA-Storage	HCNA-Design
资深工程师级	HCNP-R&S (HCDP)	HCNP-Carrier (HCDP-Carrier)	HCNP-WLAN	HCNP-LTE	HCNP-Transmission	HCNP-Security	HCNP-UC	HCNP-CC	HCNP-VC	HCNP-Cloud	HCNP-Storage	HCNP-Design
专家级	HCIE-R&S	HCIE-Carrier	HCIE-WLAN	HCIE-LTE	HCIE-Transmission	HCIE-Security	HCIE-UC	HCIE-CC	HCIE-VC	HCIE-Cloud	HCIE-Storage	HCIE-Design
架构师级	HCAr											

前言

简介

本书为HCNA认证培训教程，专门适用于准备参加HCNA考试的学员。对于希望通过在华为VRP平台上进行实际操作和演练，从而加强认识和理解数据通信原理的在校学生和专业人员，本书也极具参考价值。

内容描述

本书共包含五个Module，全面地介绍了增强企业网络各种重要特性所涉及的相关技术，以及这些技术是如何在VRP上配置和实现的。

Module 1介绍了提升企业网络效率与可靠性的相关技术，内容包含链路聚合、VLAN、GARP & GVRP以及WLAN。

Module 2介绍了企业网络远程互连时常用的WAN技术，包含HDLC、PPP、Frame Relay、PPPoE和无线3G。

Module 3介绍了基于华为路由交换产品的企业网安全技术，包含ACL、AAA、IPSec VPN和GRE。

Module 4介绍了企业网管系统的基本原理以及配置与实现，同时也介绍了华为企业网管系统eSight的诸多特性。

Module 5介绍了IPv6基础、IPv6路由协议RIPng和OSPFv3、以及DHCPv6。

本书的目的在于：结合华为的产品实现，引导读者从基础开始，循序渐进地熟

悉和掌握以路由交换技术为核心的数据通信知识。对于基础知识较为薄弱的读者，建议严格按照本书的编排内容进行顺序地阅读学习；其他读者可根据自身的情况进行有选择性地阅读学习。

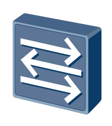
读者知识背景

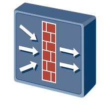
本课程为华为认证 HCNA v2.0 进阶课程，要求读者具有一定网络知识背景或相关行业经验，或者已经具备和掌握 HCNA 入门课程中的网络知识和技能。

本书常用图标


路由器


汇聚层交换机


接入层交换机


防火墙



AP


PC


便携电脑


普通服务器

电话

IP电话

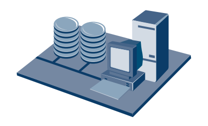

DSLAM


RADIUS服务器


邮件服务器


存储服务器

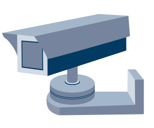

应用服务器

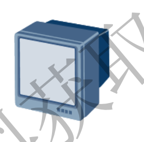

NMS


智能手机


PAD


球机


带云台的枪机


IP电视


AC

目录

Module-0

企业网络进阶


企业网络解决方案
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

随着业务的不断发展，企业对网络的要求也在不断提高。仅仅提供数据传输的基础网络已经不能满足企业业务发展的需求。如今的企业网络需要针对不同业务，提供不同的网络服务，还需要通过配置策略来应对越来越多的内部和外部的安全威胁，以保障企业网络的安全。因此，扩展现有的企业网络变得越来越有必要。

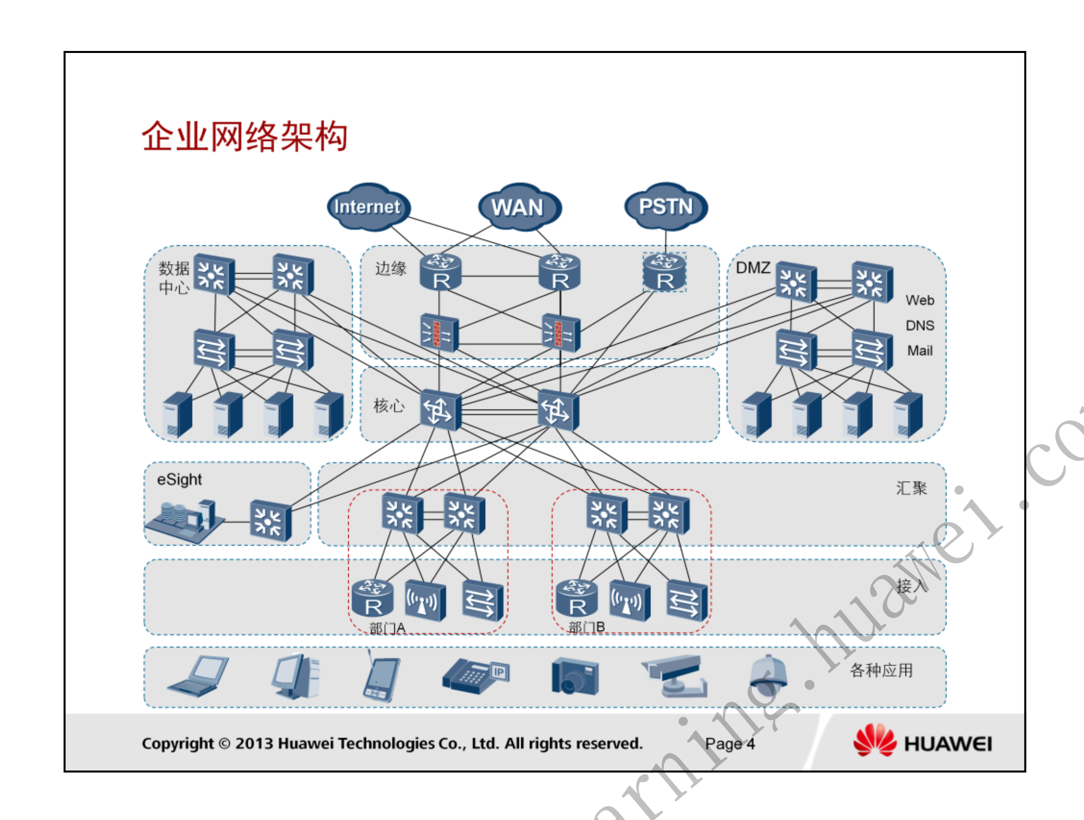




学习目标

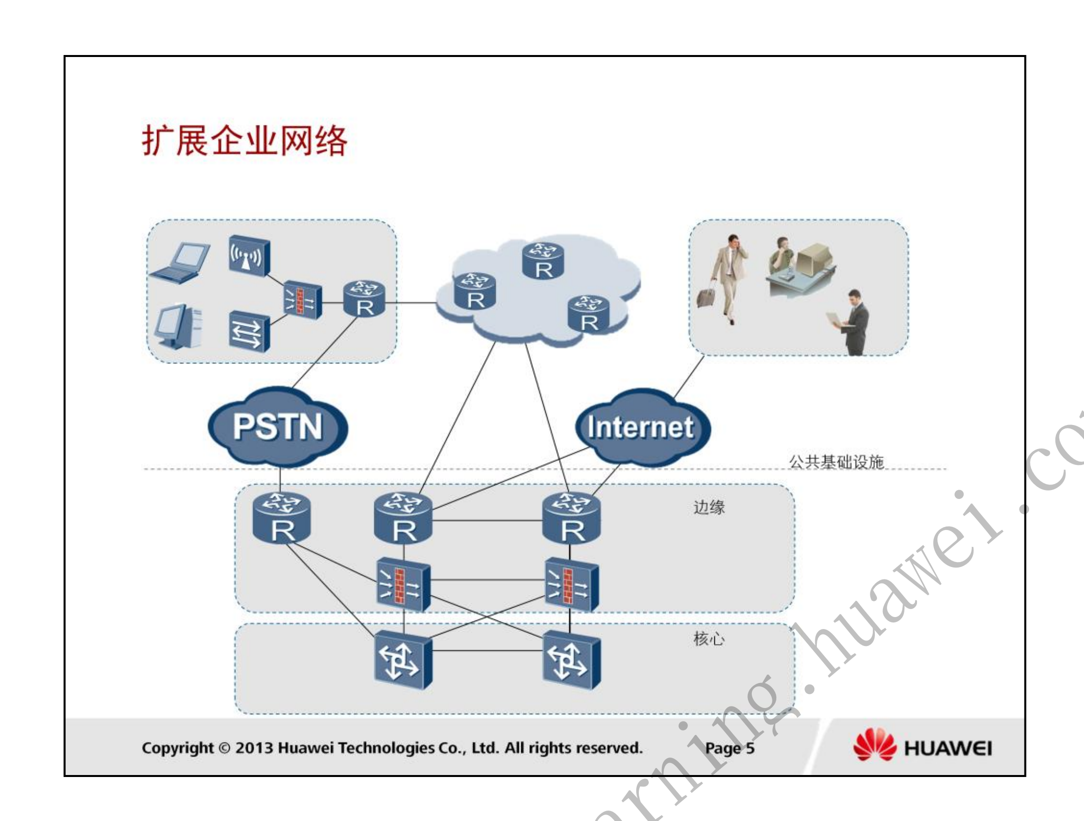
学完本课程成后，您应该能：

- 掌握企业网络的体系结构
- 掌握企业网络的业务需求

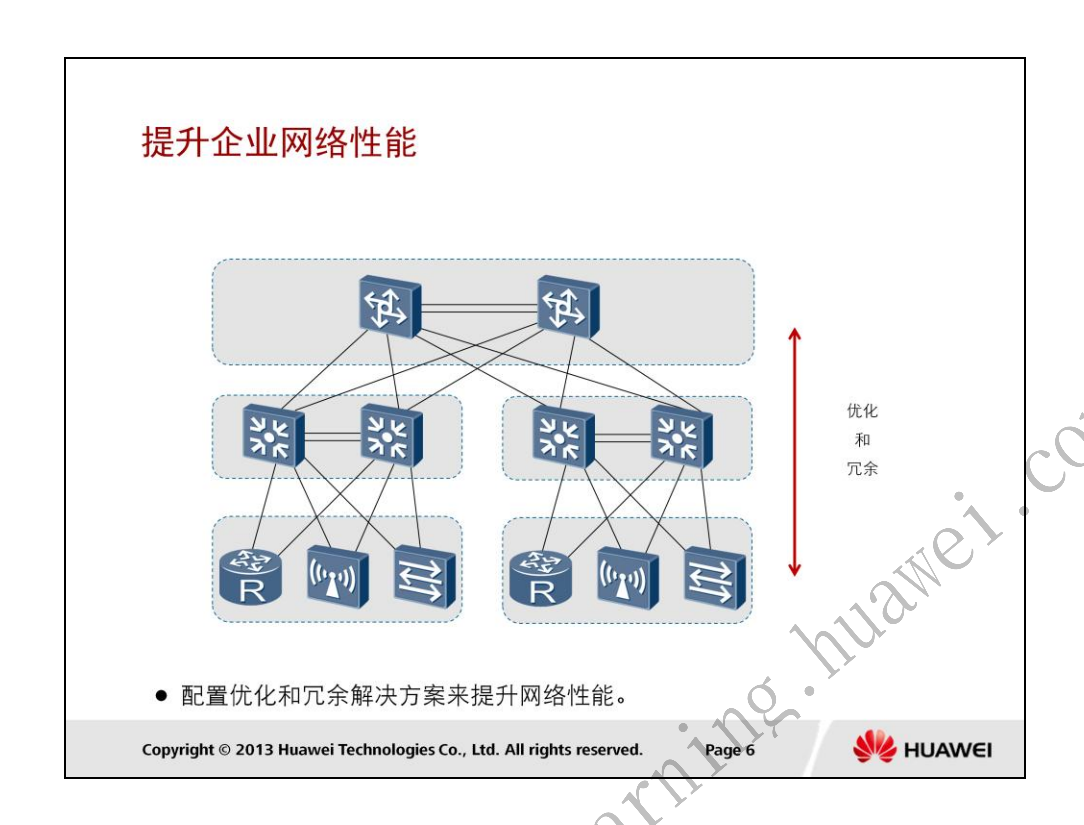


企业需要具备一个完整的网络解决方案，才能支撑各种各样的业务运转。随着业务不断发展，对企业对网络的各种需求也在不断增加。例如：用户密度可能在短时间内快速增加，用户需要移动办公，此外企业还需要有效地管理网络中不同的业务流量。

本例中描述的是一个企业网络解决方案，此方案将网络在逻辑上分为不同的区域：接入、汇聚、核心区域，数据中心区域，DMZ区域，企业边缘，网络管理区域等。此网络使用了一个三层的网络架构，包括核心层，汇聚层，接入层。将网络分为三层架构有诸多优点：每一层都有各自独立而特定的功能；使用模块化的设计，便于定位错误，简化网络拓展和维护；可以隔离一个区域的拓扑变化，避免影响其他区域。此解决方案能够支持各种应用对网络的需求，包括高密度的用户接入，移动办公，VoIP，视频会议和视频监控的使用等，满足了客户对于可扩展性，可靠性，安全性，可管理性的需求。



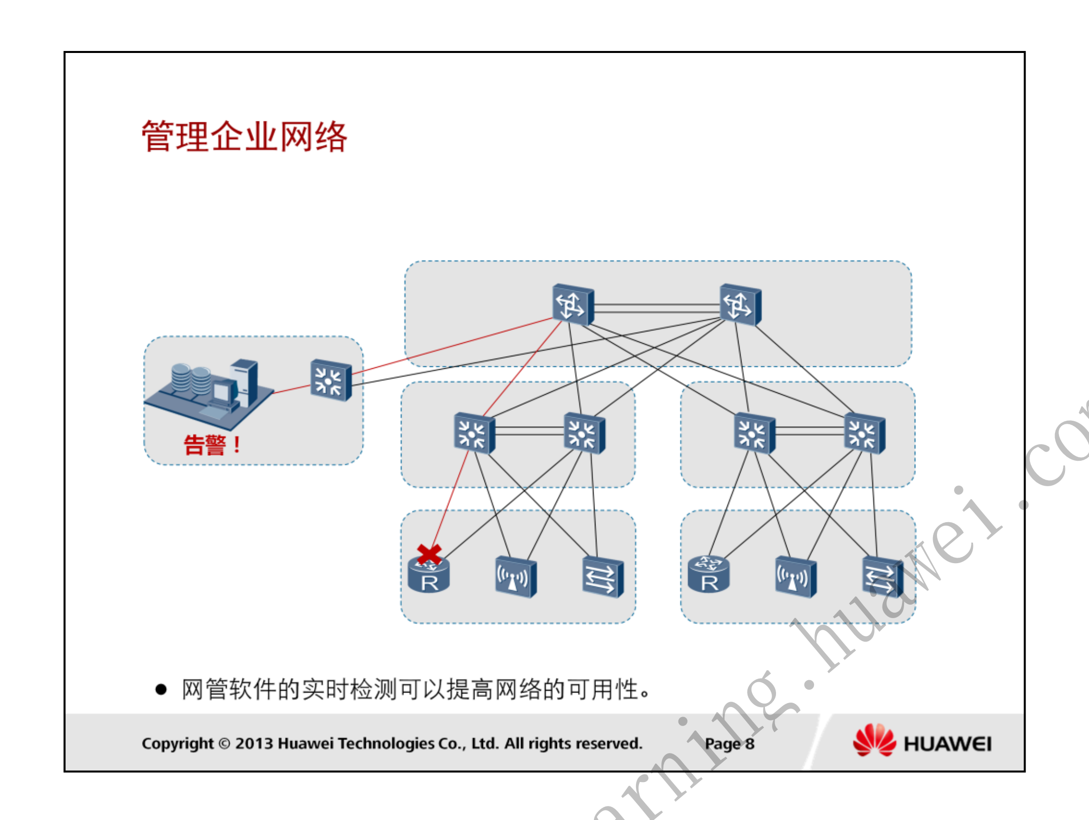
企业网络通过与电信服务供应商的网络建立连接，来支撑移动办公和分支机构网络的互联。移动办公的用户只要能够接入网络，就可以在任何时间、任何地点访问到企业内部网络。



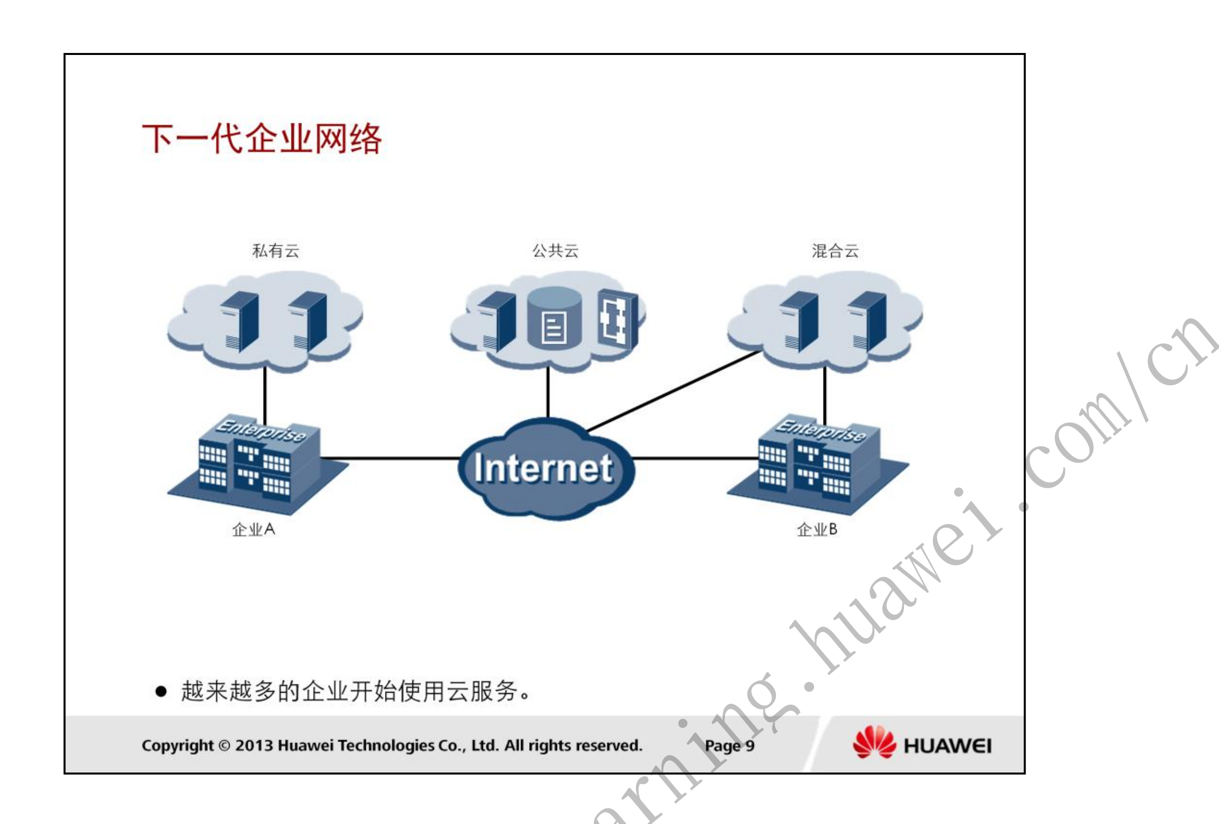
提升企业网络运作效率，需要优化网络设计。在网络中使用冗余架构，可以尽可能地保证无论任何设备或链路发生故障，用户业务都不会被影响。双节点冗余设计作为企业网络设计的一部分，增强了网络可靠性。但冗余不能过度使用，因为太多的冗余节点难以维护，并且增加了整体开销。



网络安全在企业网络中变得日益重要。TCP/IP协议簇在建立之初并没有考虑到安全问题，因此，企业网络亟需能够应对内外两种安全威胁的解决方案，用来对抗IP网络中日益增长的安全威胁。华为网络安全解决方案覆盖了终端安全管理，业务安全控制，网络攻击防护三大方面。



华为开发的eSight网管系统实现了企业资源、服务和用户的统一管理，并且允许它们进行智能互动。此外，eSight还能够管理来自其它厂商的设备，比如华三、思科和中兴的网络设备以及IBM、惠普和Sun Microsystems的IT设备。

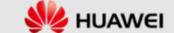


随着行业的不断发展，出现了新一代企业解决方案，即云解决方案。云解决方案为业务运行所需的基础设施、平台及软件提供了云服务，以此来满足每个客户的需求。企业需要建设云解决方案所需的数据中心和基础设施，需要使用虚拟化和存储等技术，推动企业把云解决方案运用到所有业务中，从而满足客户持续增长的业务需求。



总结

- 在企业网络中的DMZ有什么功能?
- 核心层在企业网络中扮演什么样的角色?



1. DMZ(Demilitarized Zone)即非军事话区域，DMZ可以理解为一个不同于外网或内网的特殊网络区域，一般用来存放企业的各种公用服务器，比如Web、Mail、FTP等。
2. 核心层用于高速转发企业网络内部不同区域间的流量，将内部流量转发到外部区域，或将外部流量转发到企业内部。核心层设备必须具备很高的处理和转发性能。


谢谢
www.huawei.com

Module-1

提升企业网络的效率与可靠性


链路聚合
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

随着网络规模不断扩大，用户对骨干链路的带宽和可靠性提出了越来越高的要求。在传统技术中，常用更换高速率的接口板或更换支持高速率接口板的设备的方式来增加带宽，但这种方案需要付出高额的费用，而且不够灵活。

采用链路聚合技术可以在不进行硬件升级的条件下，通过将多个物理接口捆绑为一个逻辑接口，来达到增加链路带宽的目的。在实现增大带宽目的的同时，链路聚合采用备份链路的机制，可以有效的提高设备之间链路的可靠性。



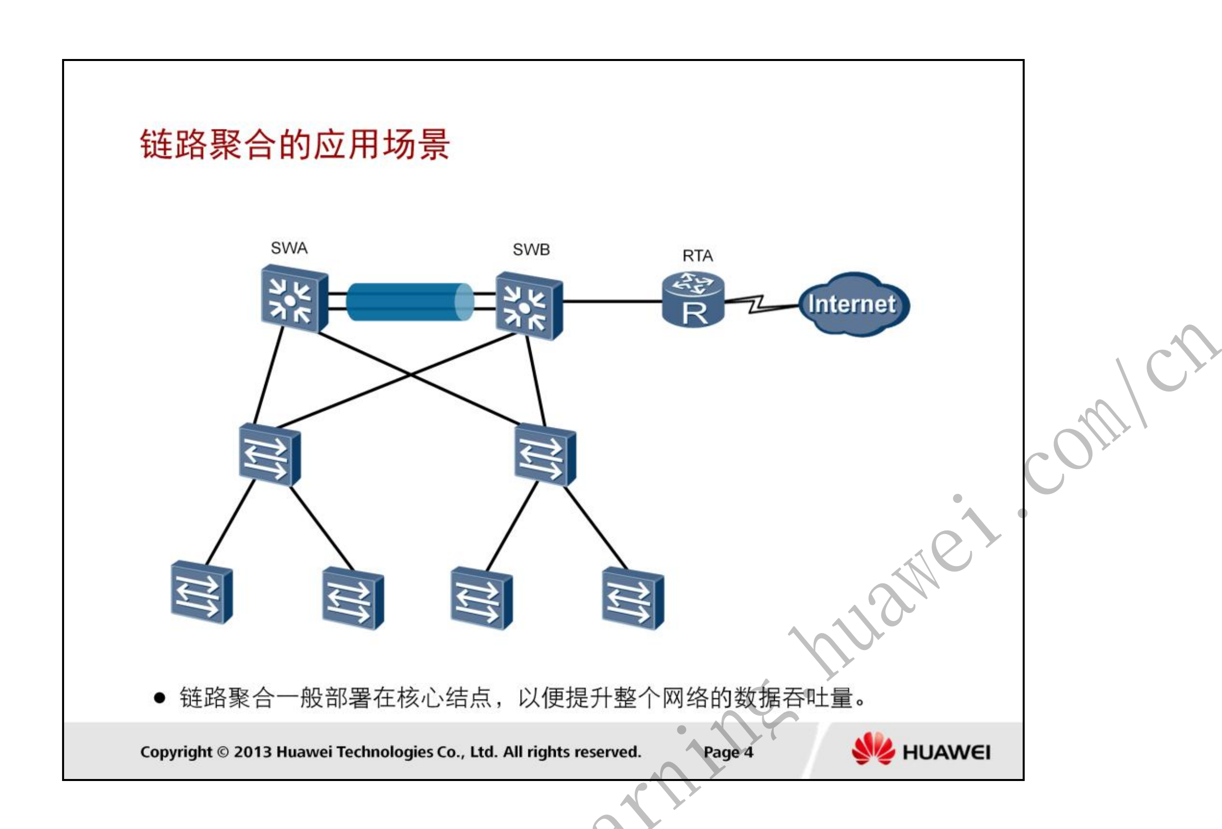


学习目标

学完本课程后，您应该能：

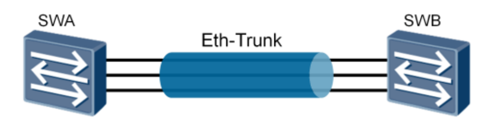
- 掌握链路聚合的原理
- 掌握链路聚合的配置

HUAWEI



在企业网络中，所有设备的流量在转发到其他网络前都会汇聚到核心层，再由核心区设备转发到其他网络，或者转发到外网。因此，在核心层设备负责数据的高速交换时，容易发生拥塞。在核心层部署链路聚合，可以提升整个网络的数据吞吐量，解决拥塞问题。本示例中，两台核心交换机SWA和SWB之间通过两条成员链路互相连接，通过部署链路聚合，可以确保SWA和SWB之间的链路不会产生拥塞。

链路聚合



- 链路聚合能够提高链路带宽，增强网络可用性，支持负载分担。





链路聚合是把两台设备之间的多条物理链路聚合在一起，当做一条逻辑链路来使用。这两台设备可以是一对路由器，一对交换机，或者是一台路由器和一台交换机。一条聚合链路可以包含多条成员链路，在ARG3系列路由器和X7系列交换机上默认最多为8条。

链路聚合能够提高链路带宽。理论上，通过聚合几条链路，一个聚合口的带宽可以扩展为所有成员口带宽的总和，这样就有效地增加了逻辑链路的带宽。

链路聚合为网络提供了高可靠性。配置了链路聚合之后，如果一个成员接口发生故障，该成员口的物理链路会把流量切换到另一条成员链路上。

链路聚合还可以在一个聚合口上实现负载均衡，一个聚合口可以把流量分散到多个不同的成员口上，通过成员链路把流量发送到同一个目的地，将网络产生拥塞的可能性降到最低。

链路聚合模式

SWA SWB
手工负载分担模式

SWA SWB
LACP模式

Active Backup

- 手工负载分担模式下所有活动接口都参与数据的转发，分担负载流量。
- LACP模式支持链路备份。

 Page 6 HUAWEI

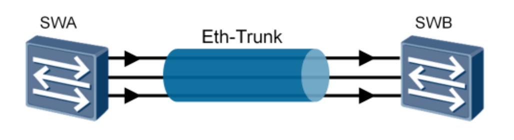
链路聚合包含两种模式：手动负载均衡模式和静态LACP（Link Aggregation Control Protocol）模式。

手工负载分担模式下，Eth-Trunk的建立、成员接口的加入由手工配置，没有链路聚合控制协议的参与。该模式下所有活动链路都参与数据的转发，平均分担流量，因此称为负载分担模式。如果某条活动链路故障，链路聚合组自动在剩余的活动链路中平均分担流量。当需要在两个直连设备间提供一个较大的链路带宽而设备又不支持LACP协议时，可以使用手工负载分担模式。ARG3系列路由器和X7系列交换机可以基于目的MAC地址，源MAC地址，或者基于源MAC地址和目的MAC地址，源IP地址，目的IP地址，或者基于源IP地址和目的IP地址进行负载均衡。

在静态LACP模式中，链路两端的设备相互发送LACP报文，协商聚合参数。协商完成后，两台设备确定活动接口和非活动接口。在静态LACP模式中，需要手动创建一个Eth-Trunk口，并添加成员口。LACP协商选举活动接口和非活动接口。静态LACP模式也叫M:N模式。M代表活动成员链路，用于在负载均衡模式中转发数据。N代表非活动链路，用于冗余备份。如果一条活动链路发生故障，该链路传输的数据被切换到一条优先级最高的备份链路上，这条备份链路转变为活动状态。

两种链路聚合模式的主要区别是：在静态LACP模式中，一些链路充当备份链路。在手动负载均衡模式中，所有的成员口都处于转发状态。

数据流控制



Duplex Mode: Full
Speed: 1000

Duplex Mode: Full
Speed: 1000

- Eth-Trunk链路两端相连的物理接口的数量、速率、双工方式、流控方式必须一致。



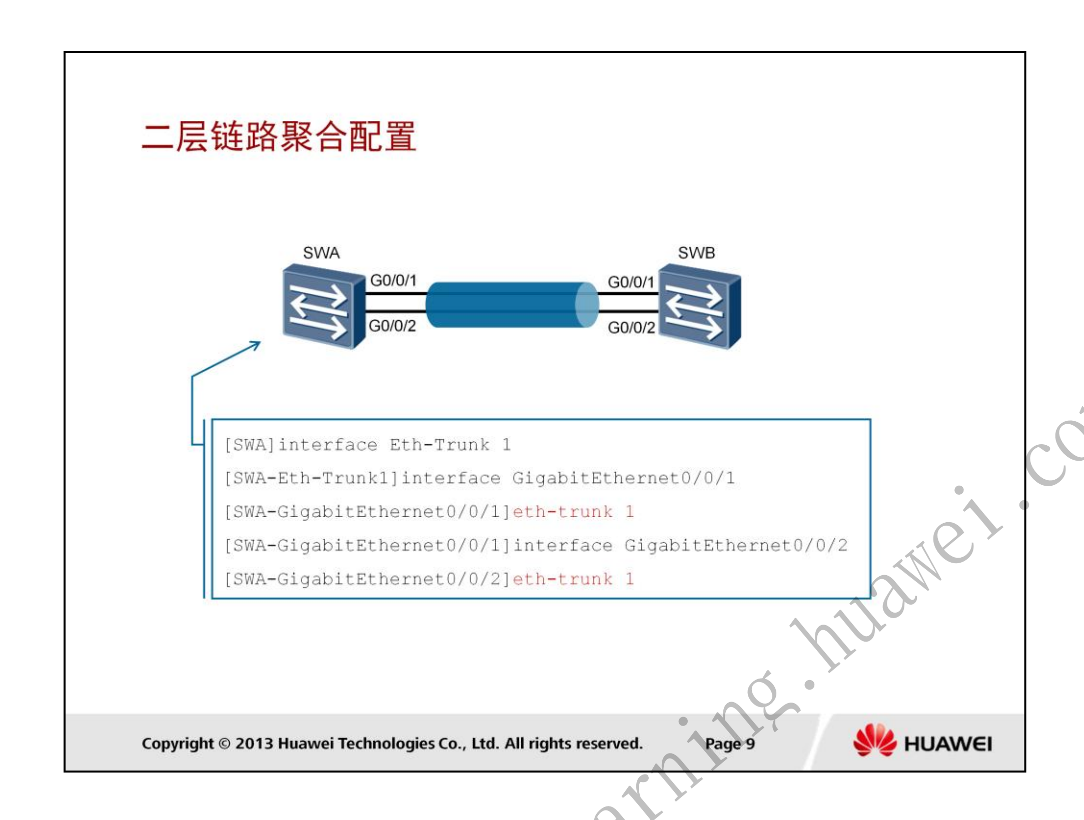
在一个聚合口中，聚合链路两端的物理口（即成员口）的所有参数必须一致，包括物理口的数量，传输速率，双工模式和流量控制模式。成员口可以是二层接口或三层接口。

数据流在聚合链路上传输，数据顺序必须保持不变。一个数据流可以看做是一组MAC地址和IP地址相同的帧。例如，两台设备间的Telnet或FTP连接可以看做一个数据流。如果未配置链路聚合，只是用一条物理链路来传输数据，那么一个数据流中的帧总是能按正确的顺序到达目的地。配置了链路聚合后，多条物理链路被绑定成一条聚合链路，一个数据流中的帧通过不同的物理链路传输。如果第一个帧通过一条物理链路传输，第二个帧通过另外一条物理链路传输，这样一来同一数据流的第二个数据帧就有可能比第一个数据帧先到达对端设备，从而产生接收数据包乱序的情况。

为了避免这种情况的发生，Eth-Trunk采用逐流负载分担的机制，这种机制把数据帧中的地址通过HASH算法生成HASH-KEY值，然后根据这个数值在Eth-Trunk转发表中寻找对应的出接口，不同的MAC或IP地址HASH得出的HASH-KEY值不同，从而出接口也就不同，这样既保证了同一数据流的帧在同一条物理链路转发，又实现了流量在聚合组内各物理链路上的负载分担，即逐流的负载分担。逐流负载分担能保证包的顺序，但不能保证带宽利用率。

负载分担的类型主要包括以下几种，用户可以根据具体应用选择不同的负载分担类型。

1. 根据报文的源MAC地址进行负载分担；
2. 根据报文的目的MAC地址进行负载分担；
3. 根据报文的源IP地址进行负载分担；
4. 根据报文的目的IP地址进行负载分担；
5. 根据报文的源MAC地址和目的MAC地址进行负载分担；
6. 根据报文的源IP地址和目的IP地址进行负载分担；
7. 根据报文的VLAN、源物理端口等对L2、IPv4、IPv6和MPLS报文进行增强型负载分担。



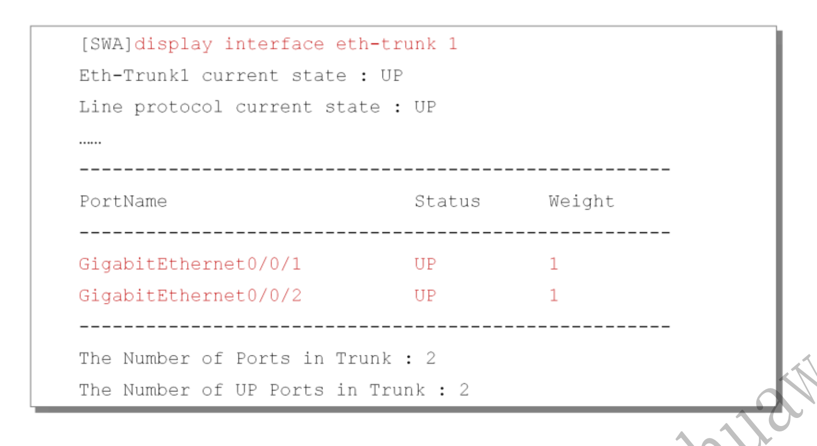
本例中，通过执行**interface Eth-trunk** *<trunk-id>*命令配置链路聚合。这条命令创建了一个Eth-Trunk口，并且进入该Eth-Trunk口视图。*trunk-id*用来唯一标识一个Eth-Trunk口，该参数的取值可以是0到63之间的任何一个整数。如果指定的Eth-Trunk口已经存在，执行**interface eth-trunk**命令会直接进入该Eth-Trunk口视图。

配置Eth-Trunk口和成员口，需要注意以下规则：

1. 只能删除不包含任何成员口的Eth-Trunk口。
2. 把接口加入Eth-Trunk口时，二层Eth-Trunk口的成员口必须是二层接口，三层Eth-Trunk口的成员口必须是三层接口。
3. 一个Eth-Trunk口最多可以加入8个成员口。
4. 加入Eth-Trunk口的接口必须是hybrid接口（默认的接口类型）。
5. 一个Eth-Trunk口不能充当其他Eth-Trunk口的成员口。
6. 一个以太接口只能加入一个Eth-Trunk口。如果把一个以太接口加入另一个Eth-Trunk口，必须先把该以太接口从当前所属的Eth-Trunk口中删除。
7. 一个Eth-Trunk口的成员口类型必须相同。例如，一个快速以太口（FE口）和一个千兆以太口（GE口）不能加入同一个Eth-Trunk。
8. 位于不同接口板（LPU）上的以太口可以加入同一个Eth-Trunk口。如果一个对端接口直接和本端Eth-Trunk口的一个成员口相连，该对端接口也必须加入一个Eth-Trunk口。否则两端无法通信。

9. 如果成员口的速率不同，速率较低的接口可能会拥塞，报文可能会被丢弃。
10. 接口加入Eth-Trunk口后，Eth-Trunk口学习MAC地址，成员口不再学习。

查看链路聚合信息



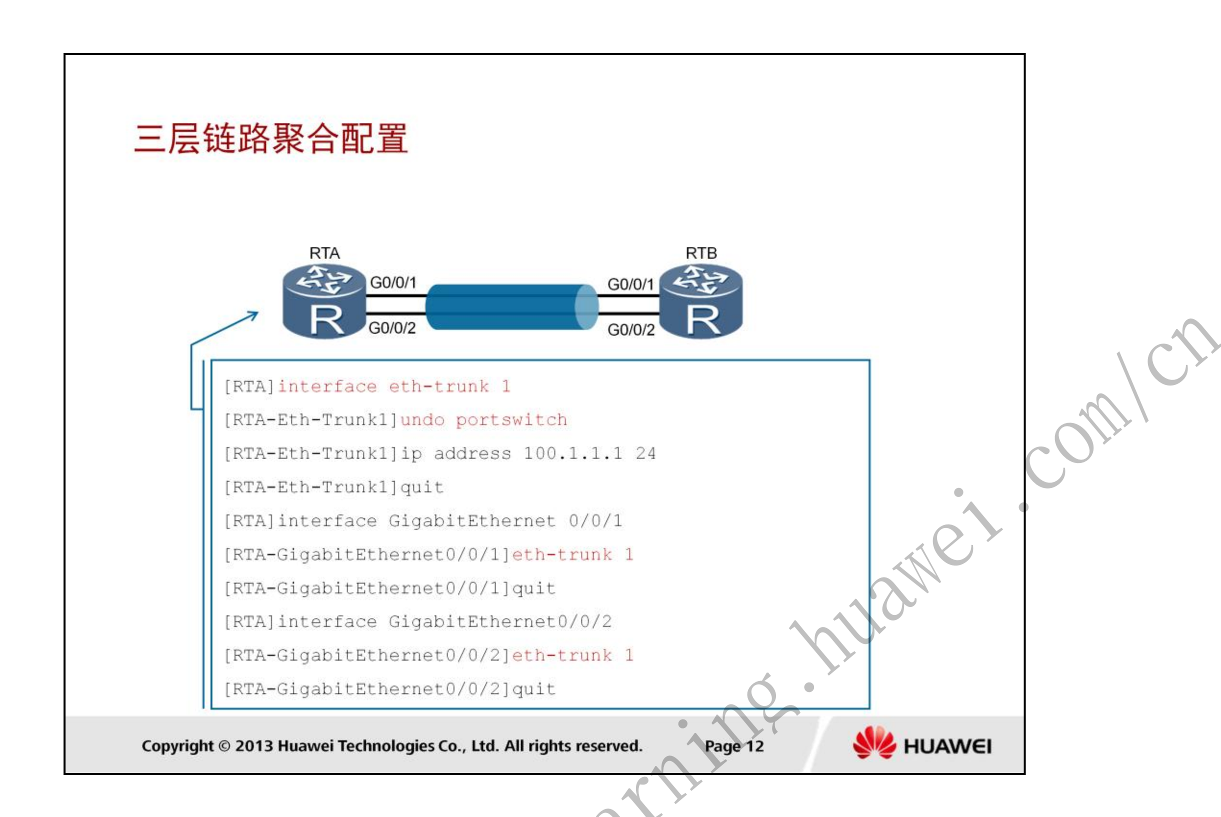
```
[SWA]display interface eth-trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
……
--------------------------------------------------------
PortName                      Status      Weight
--------------------------------------------------------
GigabitEthernet0/0/1          UP          1
GigabitEthernet0/0/2          UP          1
--------------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

- 两个成员接口已经被绑定到Eth-trunk 1。

 Page 11

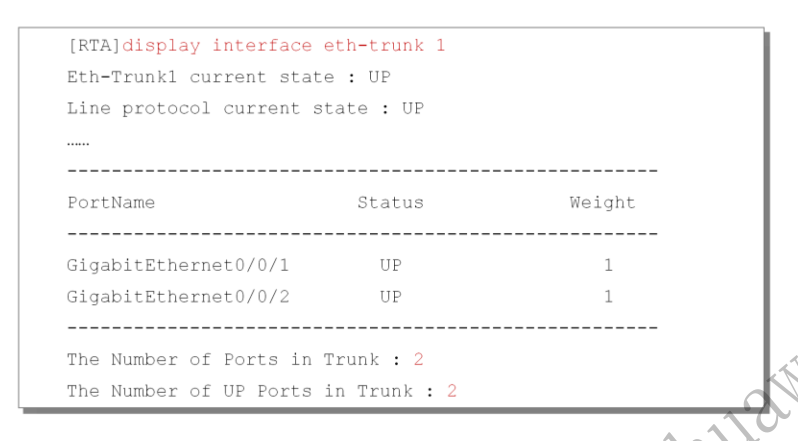


执行**display interface eth-trunk** *<trunk-id>*命令，可以确认两台设备间是否已经成功实现链路聚合。也可以使用这条命令收集流量统计数据，定位接口故障。如果Eth-Trunk口处于UP状态，表明接口正常运行。如果接口处于Down状态，表明所有成员口物理层发生故障。如果管理员手动关闭端口，接口处于Administratively DOWN状态。可以通过接口状态的改变发现接口故障，所有接口正常情况下都应处于Up状态。



如果要在路由器上配置三层链路聚合，需要首先创建Eth-Trunk接口，然后在Eth-Trunk逻辑口上执行**undo portswitch**命令，把聚合链路从二层转为三层链路。执行**undo portswitch**命令后，可以为Eth-Trunk逻辑口分配一个IP地址。

查看链路聚合信息



```
[RTA]display interface eth-trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
……
-----------------------------------------------------
PortName                  Status            Weight
-----------------------------------------------------
GigabitEthernet0/0/1        UP                 1
GigabitEthernet0/0/2        UP                 1
-----------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

- 两个成员接口已经被绑定到Eth-trunk 1。

Page 13



执行**display interface eth-trunk** *<trunk-id>*命令，可以确认两台设备间是否已经成功实现链路聚合。也可以使用这条命令收集流量统计数据，定位接口故障。如果Eth-Trunk口处于UP状态，表明接口正常运行。如果接口处于Down状态，表明所有成员口物理层发生故障。如果管理员手动关闭端口，接口处于Administratively DOWN状态。可以通过接口状态的改变发现接口故障，所有接口正常情况下都应处于Up状态。



总结

- 如果一个管理员希望将千兆以太口和百兆以太口加入同一个Eth-trunk，会发生什么？
- 哪种链路聚合方法可以使用链路备份？





1. 一个快速以太口（FE口）和一个千兆以太口（GE口）不能加入同一个Eth-Trunk。如果将两个不同类型的接口加入到同一个Eth-Trunk口，设备会提示发生错误。
2. 只有LACP模式支持备份成员链路。如需建立备份链路，应使用LACP模式的链路聚合。


谢谢
www.huawei.com


VLAN原理和配置
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

随着网络中计算机的数量越来越多，传统的以太网络开始面临冲突严重、广播泛滥以及安全性无法保障等各种问题。

VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的局域网在逻辑上划分成多个广播域的技术。通过在交换机上配置VLAN，可以实现在同一个VLAN内的用户可以进行二层互访，而不同VLAN间的用户被二层隔离。这样既能够隔离广播域，又能够提升网络的安全性。



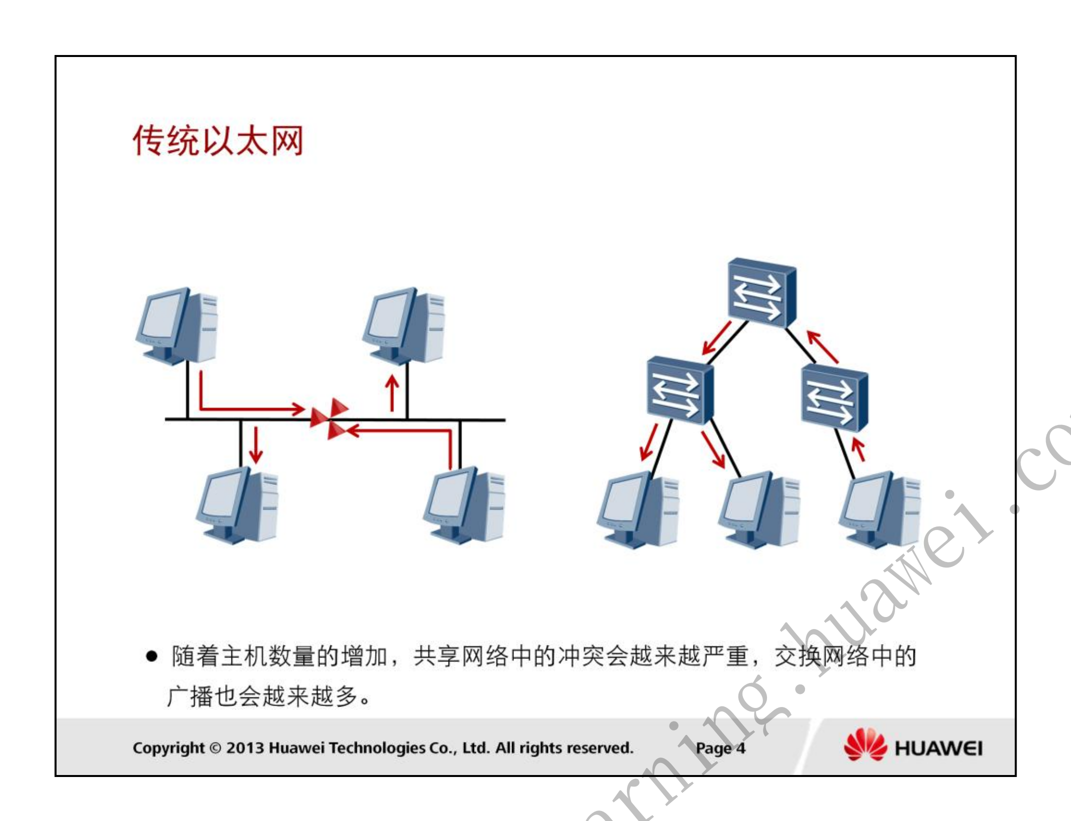


学习目标

学完本课程后，您应该能：

- 理解VLAN的工作原理
- 掌握VLAN的基本配置





早期的局域网LAN技术是基于总线型结构的，它存在以下主要问题:

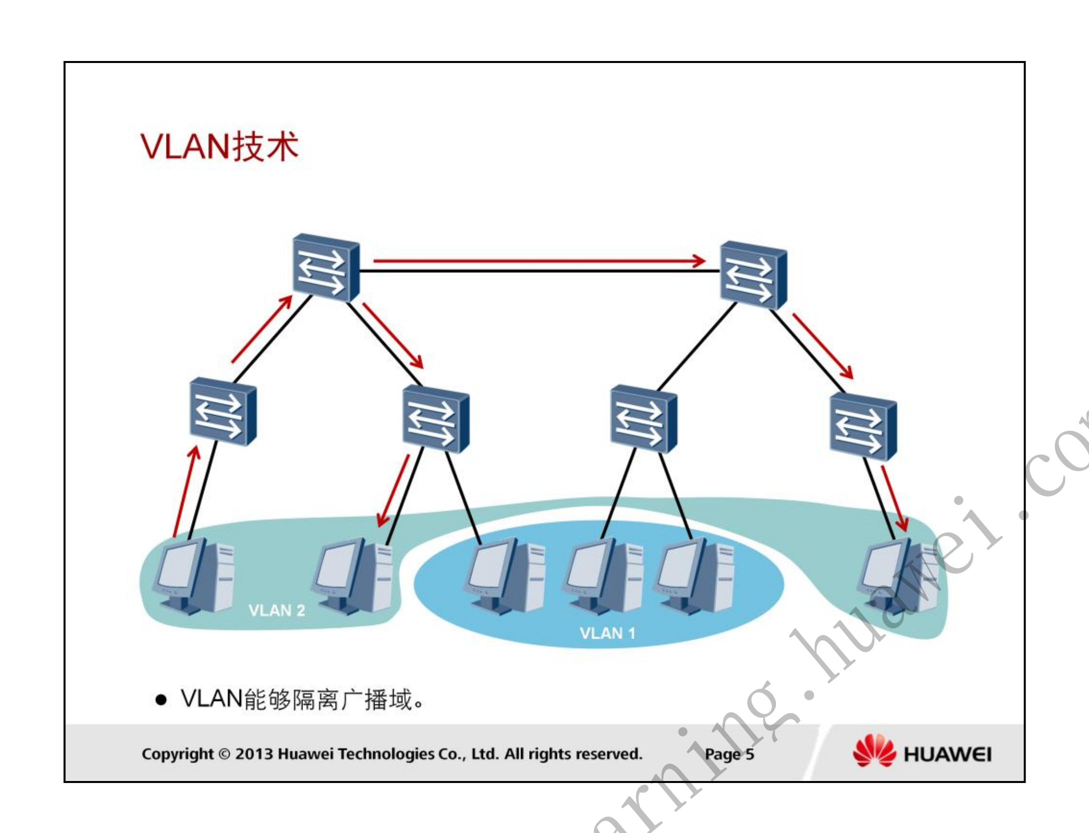
1. 若某时刻有多个节点同时试图发送消息，那么它们将产生冲突。
2. 从任意节点发出的消息都会被发送到其他节点，形成广播。
3. 所有主机共享一条传输通道，无法控制网络中的信息安全。

这种网络构成了一个冲突域，网络中计算机数量越多，冲突越严重，网络效率越低。同时，该网络也是一个广播域，当网络中发送信息的计算机数量越多时，广播流量将会耗费大量带宽。

因此，传统局域网不仅面临冲突域太大和广播域太大两大难题，而且无法保障传输信息的安全。

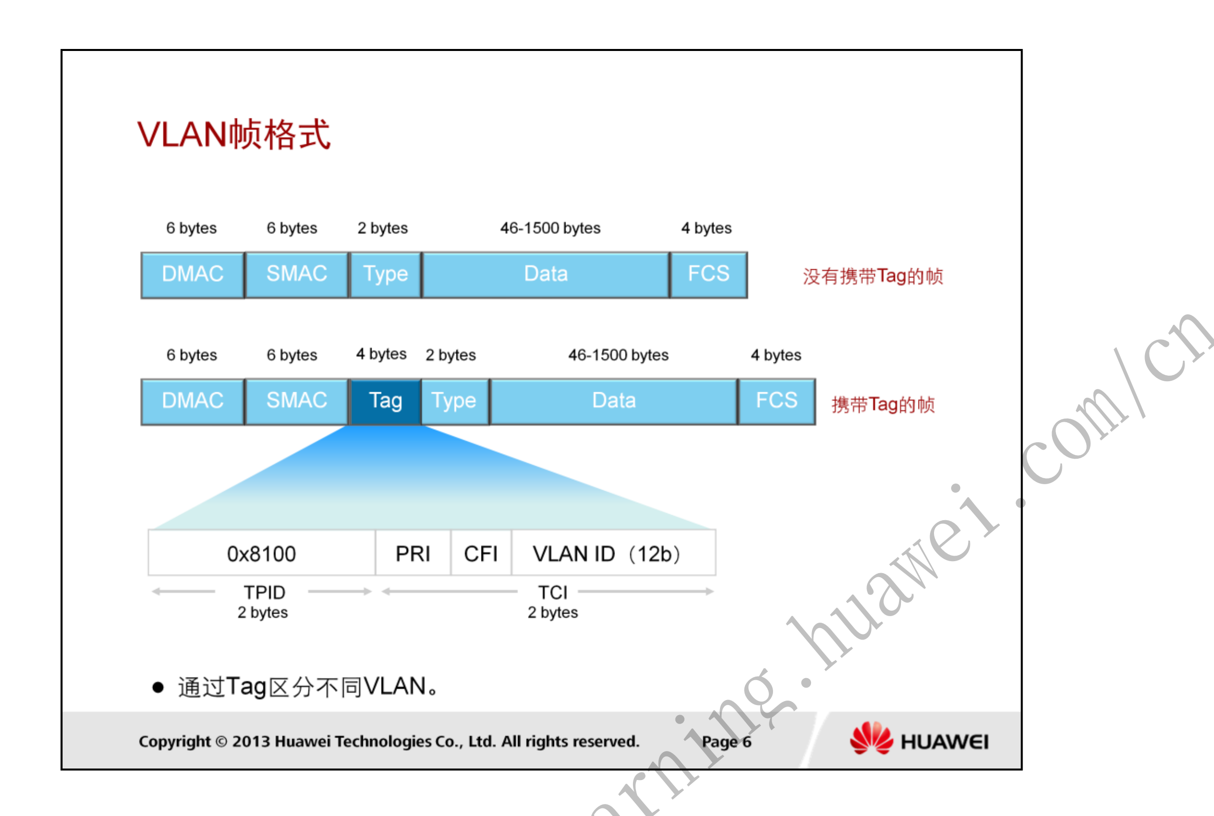
为了扩展传统LAN，以接入更多计算机，同时避免冲突的恶化，出现了网桥和二层交换机，它们能有效隔离冲突域。网桥和交换机采用交换方式将来自入端口的信息转发到出端口上，克服了共享网络中的冲突问题。但是，采用交换机进行组网时，广播域和信息安全问题依旧存在。

为限制广播域的范围，减少广播流量，需要在没有二层互访需求的主机之间进行隔离。路由器是基于三层IP地址信息来选择路由和转发数据的，其连接两个网段时可以有效抑制广播报文的转发，但成本较高。因此，人们设想在物理局域网上构建多个逻辑局域网，即VLAN。



VLAN技术可以将一个物理局域网在逻辑上划分成多个广播域，也就是多个VLAN。VLAN技术部署在数据链路层，用于隔离二层流量。同一个VLAN内的主机共享同一个广播域，它们之间可以直接进行二层通信。而VLAN间的主机属于不同的广播域，不能直接实现二层互通。这样，广播报文就被限制在各个相应的VLAN内，同时也提高了网络安全性。

本例中，原本属于同一广播域的主机被划分到了两个VLAN中，即，VLAN1和VLAN2。VLAN内部的主机可以直接在二层互相通信，VLAN1和VLAN2之间的主机无法直接实现二层通信。



VLAN标签长4个字节，直接添加在以太网帧头中，IEEE802.1Q文档对VLAN标签作出了说明。

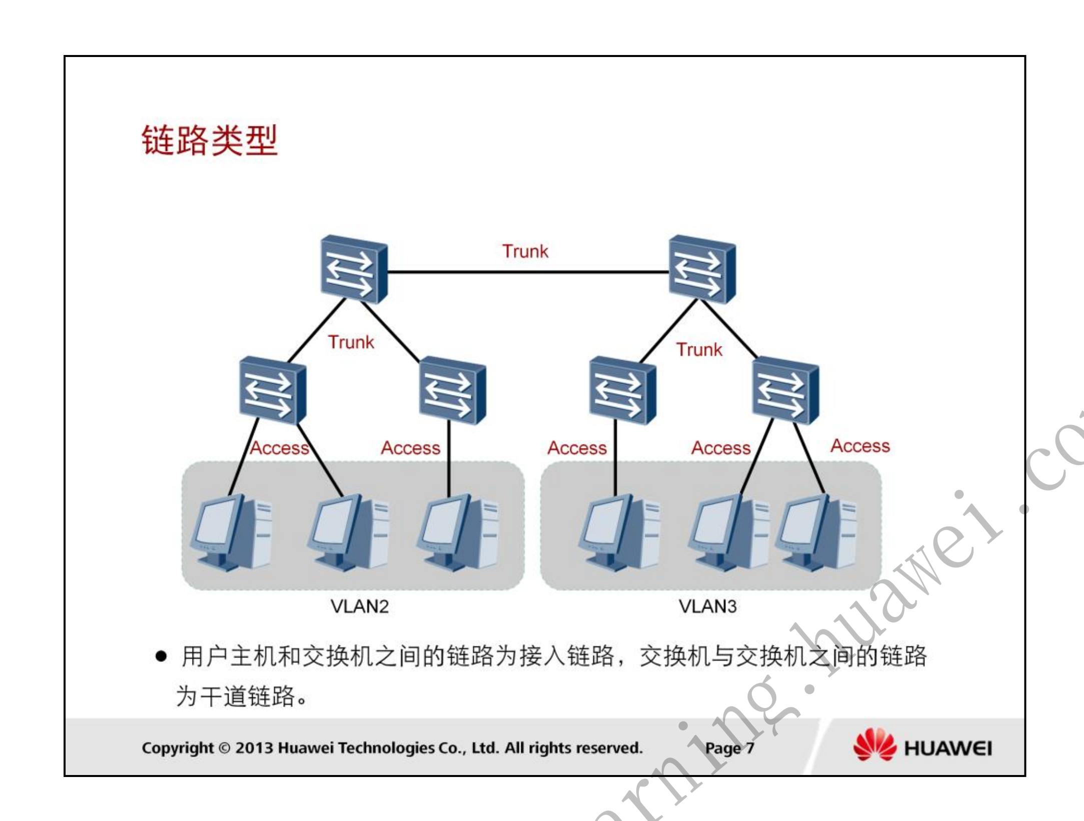
TPID：Tag Protocol Identifier，2字节，固定取值，0x8100，是IEEE定义的新类型，表明这是一个携带802.1Q标签的帧。如果不支持802.1Q的设备收到这样的帧，会将其丢弃。

TCI：Tag Control Information，2字节。帧的控制信息，详细说明如下：

1. Priority：3比特，表示帧的优先级，取值范围为0～7，值越大优先级越高。当交换机阻塞时，优先发送优先级高的数据帧。
2. CFI：Canonical Format Indicator，1比特。CFI表示MAC地址是否是经典格式。CFI为0说明是经典格式，CFI为1表示为非经典格式。用于区分以太网帧、FDDI（Fiber Distributed Digital Interface）帧和令牌环网帧。在以太网中，CFI的值为0。
3. VLAN Identifier：VLAN ID，12比特，在X7系列交换机中，可配置的VLAN ID取值范围为0～4095，但是0和4095在协议中规定为保留的VLAN ID，不能给用户使用。

在现有的交换网络环境中，以太网的帧有两种格式：

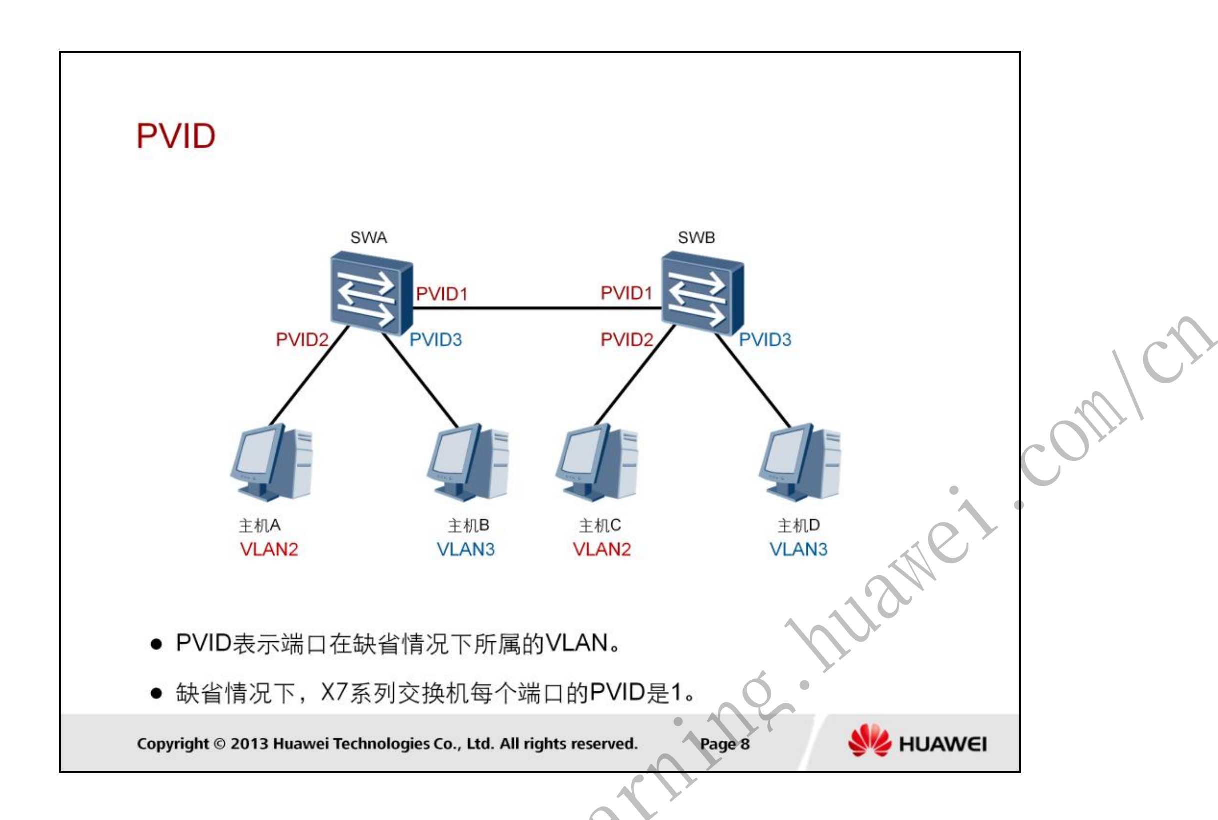
没有加上VLAN标记的标准以太网帧（untagged frame）；有VLAN标记的以太网帧（tagged frame）。



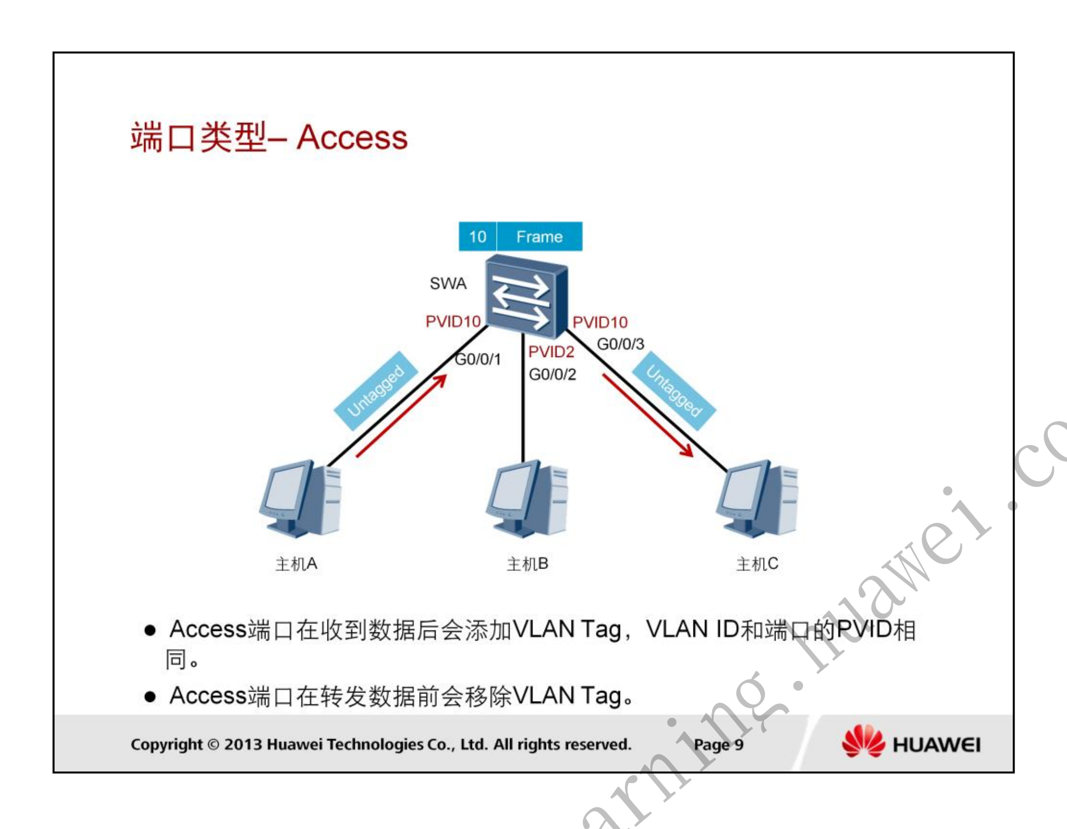
VLAN链路分为两种类型：Access链路和Trunk链路。

接入链路（Access Link）：连接用户主机和交换机的链路称为接入链路。如本例所示，图中主机和交换机之间的链路都是接入链路。

干道链路（Trunk Link）：连接交换机和交换机的链路称为干道链路。如本例所示，图中交换机之间的链路都是干道链路。干道链路上通过的帧一般为带Tag的VLAN帧。



PVID即Port VLAN ID，代表端口的缺省VLAN。交换机从对端设备收到的帧有可能是Untagged的数据帧，但所有以太网帧在交换机中都是以Tagged的形式来被处理和转发的，因此交换机必须给端口收到的Untagged数据帧添加上Tag。为了实现此目的，必须为交换机配置端口的缺省VLAN。当该端口收到Untagged数据帧时，交换机将给它加上该缺省VLAN的VLAN Tag。



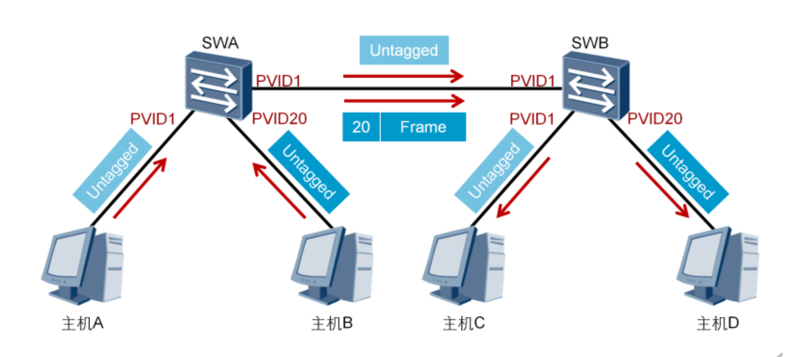
Access端口是交换机上用来连接用户主机的端口，它只能连接接入链路，并且只能允许唯一的VLAN ID通过本端口。

Access端口收发数据帧的规则如下：

1. 如果该端口收到对端设备发送的帧是untagged（不带VLAN标签），交换机将强制加上该端口的PVID。如果该端口收到对端设备发送的帧是tagged（带VLAN标签），交换机会检查该标签内的VLAN ID。当VLAN ID与该端口的PVID相同时，接收该报文。当VLAN ID与该端口的PVID不同时，丢弃该报文。
2. Access端口发送数据帧时，总是先剥离帧的Tag，然后再发送。Access端口发往对端设备的以太网帧永远是不带标签的帧。

在本示例中，交换机的G0/0/1，G0/0/2，G0/0/3端口分别连接三台主机，都配置为Access端口。主机A把数据帧（未加标签）发送到交换机的G0/0/1端口，再由交换机发往其他目的地。收到数据帧之后，交换机根据端口的PVID给数据帧打上VLAN标签10，然后决定从G0/0/3端口转发数据帧。G0/0/3端口的PVID也是10，与VLAN标签中的VLAN ID相同，交换机移除标签，把数据帧发送到主机C。连接主机B的端口的PVID是2，与VLAN10不属于同一个VLAN，因此此端口不会接收到VLAN10的数据帧。

端口类型–Trunk



- 当Trunk端口收到帧时，如果该帧不包含Tag，将打上端口的PVID；如果该帧包含Tag，则不改变。
- 当Trunk端口发送帧时，该帧的VLAN ID在Trunk的允许发送列表中：若与端口的PVID相同时，则剥离Tag发送；若与端口的PVID不同时，则直接发送。

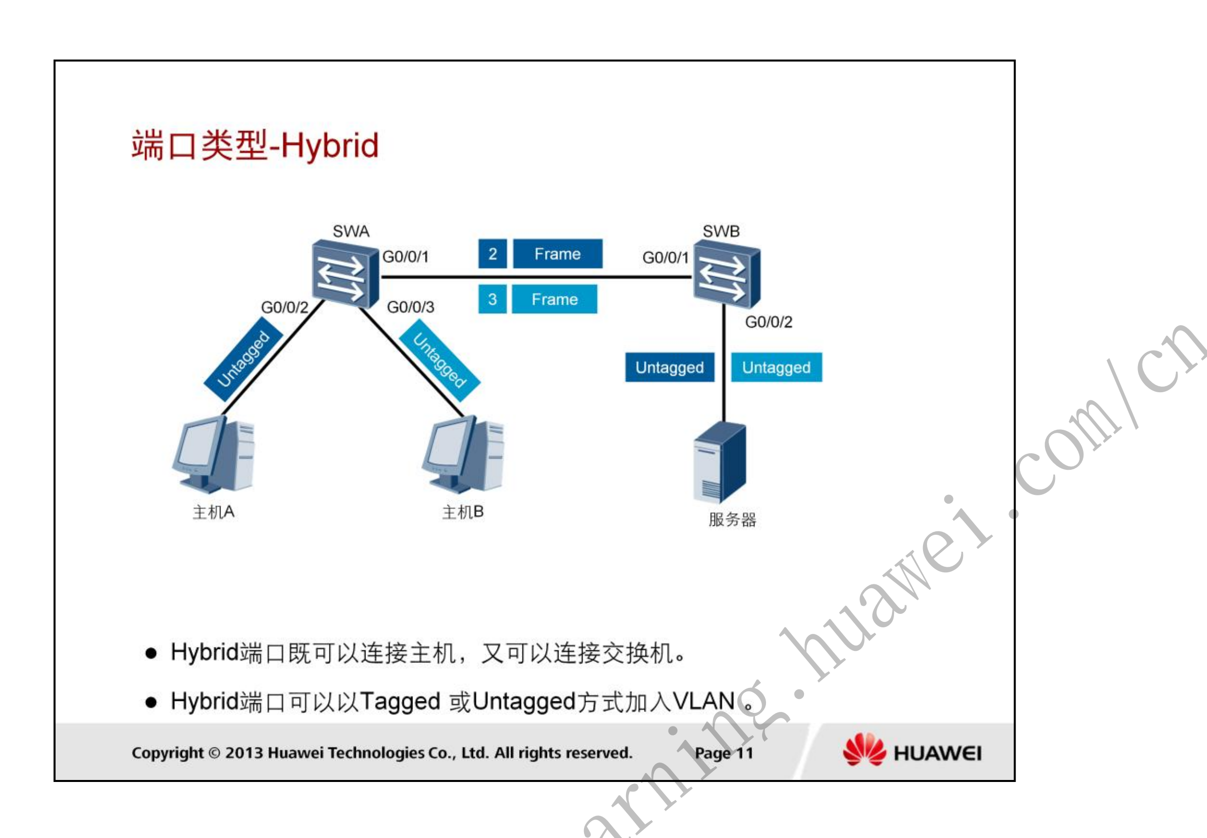
Page 10


Trunk端口是交换机上用来和其他交换机连接的端口，它只能连接干道链路。Trunk端口允许多个VLAN的帧（带Tag标记）通过。

Trunk端口收发数据帧的规则如下：

1. 当接收到对端设备发送的不带Tag的数据帧时，会添加该端口的PVID，如果PVID在允许通过的VLAN ID列表中，则接收该报文，否则丢弃该报文。当接收到对端设备发送的带Tag的数据帧时，检查VLAN ID是否在允许通过的VLAN ID列表中。如果VLAN ID在接口允许通过的VLAN ID列表中，则接收该报文。否则丢弃该报文。
2. 端口发送数据帧时，当VLAN ID与端口的PVID相同，且是该端口允许通过的VLAN ID时，去掉Tag，发送该报文。当VLAN ID与端口的PVID不同，且是该端口允许通过的VLAN ID时，保持原有Tag，发送该报文。

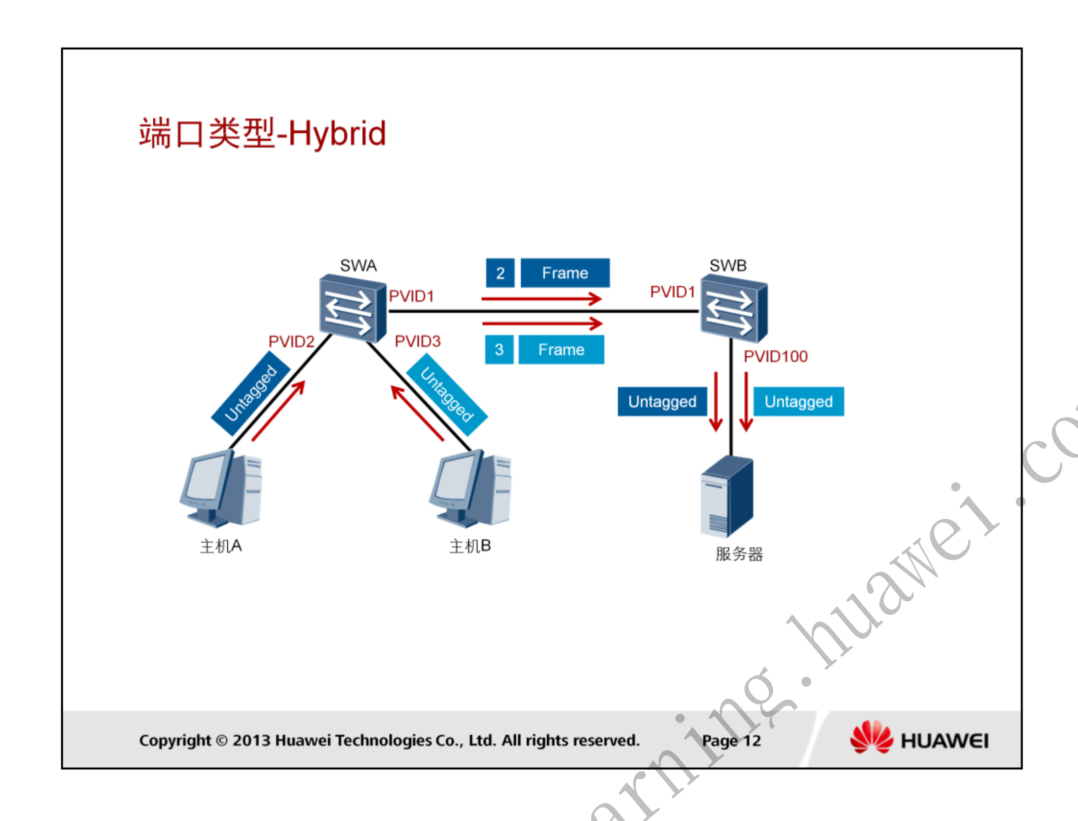
在本示例中，SWA和SWB连接主机的端口为Access端口，PVID如图所示。SWA和SWB互连的端口为Trunk端口，PVID都为1，此Trunk链路允许所有VLAN的流量通过。当SWA转发VLAN1的数据帧时会剥离VLAN标签，然后发送到Trunk链路上。而在转发VLAN20的数据帧时，不剥离VLAN标签直接转发到Trunk链路上。



Access端口发往其他设备的报文，都是Untagged数据帧，而Trunk端口仅在一种特定情况下才能发出untagged数据帧，其它情况发出的都是Tagged数据帧。

Hybrid端口是交换机上既可以连接用户主机，又可以连接其他交换机的端口。Hybrid端口既可以连接接入链路又可以连接干道链路。Hybrid端口允许多个VLAN的帧通过，并可以在出端口方向将某些VLAN帧的Tag剥掉。华为设备默认的端口类型是Hybrid。

在本示例中，要求主机A和主机B都能访问服务器，但是它们之间不能互相访问。此时交换机连接主机和服务器的端口，以及交换机互连的端口都配置为Hybrid类型。交换机连接主机A的端口的PVID是2，连接主机B的端口的PVID是3，连接服务器的端口的PVID是100。



Hybrid端口收发数据帧的规则如下：

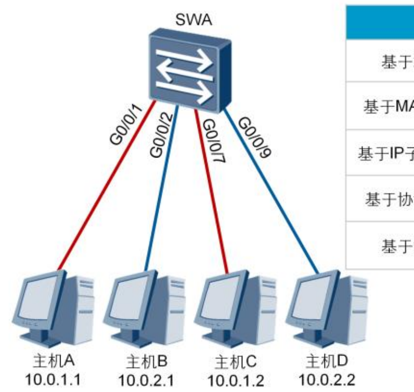
1. 当接收到对端设备发送的不带Tag的数据帧时，会添加该端口的PVID，如果PVID在允许通过的VLAN ID列表中，则接收该报文，否则丢弃该报文。当接收到对端设备发送的带Tag的数据帧时，检查VLAN ID是否在允许通过的VLAN ID列表中。如果VLAN ID在接口允许通过的VLAN ID列表中，则接收该报文，否则丢弃该报文。
2. Hybrid端口发送数据帧时，将检查该接口是否允许该VLAN数据帧通过。如果允许通过，则可以通过命令配置发送时是否携带Tag。

配置**port hybrid tagged vlan** *vlan-id*命令后，接口发送该*vlan-id*的数据帧时，不剥离帧中的VLAN Tag，直接发送。该命令一般配置在连接交换机的端口上。

配置**port hybrid untagged vlan** *vlan-id*命令后，接口在发送*vlan-id*的数据帧时，会将帧中的VLAN Tag剥离掉再发送出去。该命令一般配置在连接主机的端口上。

本例介绍了主机A和主机B发送数据给服务器的情况。在SWA和SWB互连的端口上配置了**port hybrid tagged vlan 2 3 100**命令后，SWA和SWB之间的链路上传输的都是带Tag标签的数据帧。在SWB连接服务器的端口上配置了**port hybrid untagged vlan 2 3**，主机A和主机B发送的数据会被剥离VLAN标签后转发到服务器。

VLAN划分方法



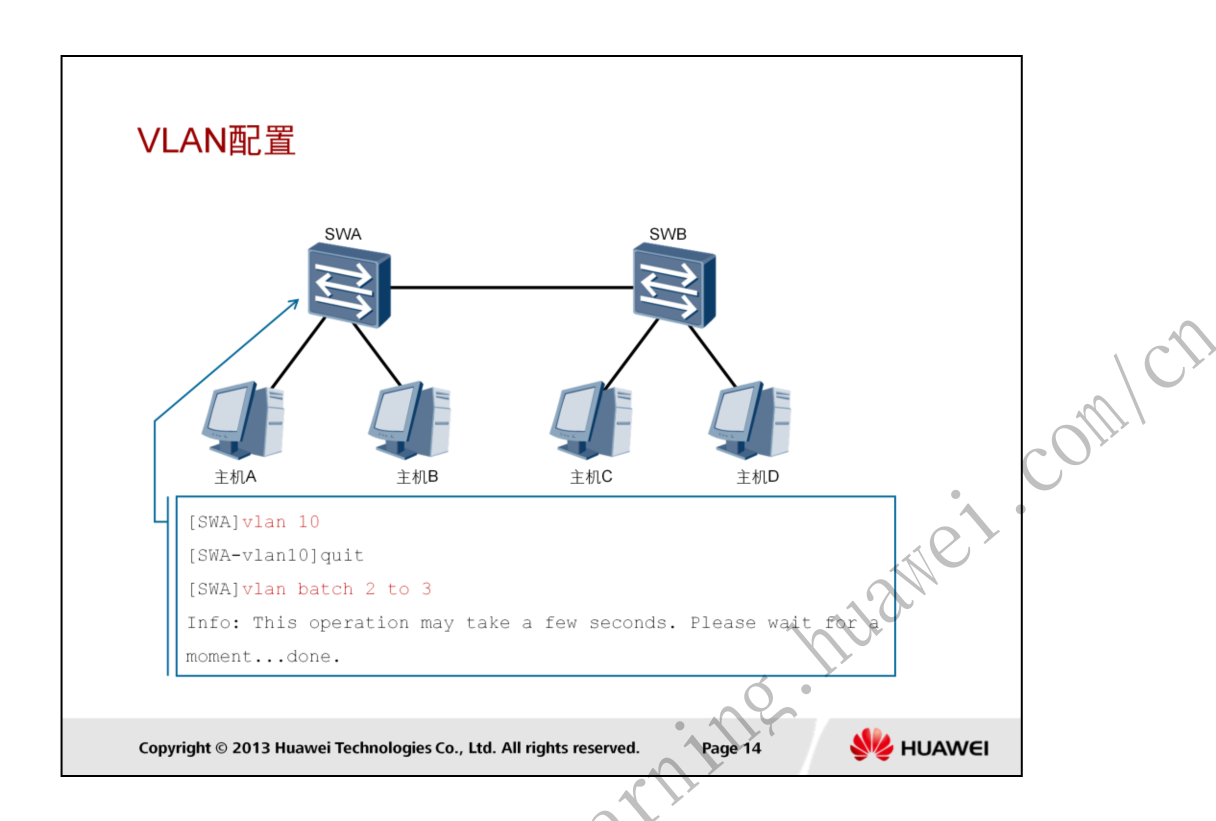
	VLAN 5	VLAN 10
基于端口	G0/0/1, G0/0/7	G0/0/2 G0/0/9
基于MAC地址	00-01-02-03-04-AA 00-01-02-03-04-CC	00-01-02-03-04-BB 00-01-02-03-04-DD
基于IP子网划分	10.0.1.*	10.0.2.*
基于协议划分	IP	IPX
基于策略	10.0.1.* + G0/0/1+ 00-01-02-03-04-AA	10.0.2.* + G0/0/2 + 00-01-02-03-04-BB

- 基于端口的VLAN划分方法在实际中最为常见。



VLAN的划分包括如下5种方法：

1. 基于端口划分：根据交换机的端口编号来划分VLAN。通过为交换机的每个端口配置不同的PVID，来将不同端口划分到VLAN中。初始情况下，X7系列交换机的端口处于VLAN1中。此方法配置简单，但是当主机移动位置时，需要重新配置VLAN。
2. 基于MAC地址划分：根据主机网卡的MAC地址划分VLAN。此划分方法需要网络管理员提前配置网络中的主机MAC地址和VLAN ID的映射关系。如果交换机收到不带标签的数据帧，会查找之前配置的MAC地址和VLAN映射表，根据数据帧中携带的MAC地址来添加相应的VLAN标签。在使用此方法配置VLAN时，即使主机移动位置也不需要重新配置VLAN。
3. 基于IP子网划分：交换机在收到不带标签的数据帧时，根据报文携带的IP地址给数据帧添加VLAN标签。
4. 基于协议划分：根据数据帧的协议类型（或协议族类型）、封装格式来分配VLAN ID。网络管理员需要首先配置协议类型和VLAN ID之间的映射关系。
5. 基于策略划分：使用几个条件的组合来分配VLAN标签。这些条件包括IP子网、端口和IP地址等。只有当所有条件都匹配时，交换机才为数据帧添加VLAN标签。另外，针对每一条策略都是需要手工配置的。



在交换机上划分VLAN时，需要首先创建VLAN。在交换机上执行**vlan** <vlan-id>命令，创建VLAN。如本例所示，执行**vlan** 10命令后，就创建了VLAN 10，并进入了VLAN 10视图。VLAN ID的取值范围是1到4094。如需创建多个VLAN，可以在交换机上执行**vlan batch** { *vlan-id1* [**to** *vlan-id2*] }命令，以创建多个连续的VLAN。也可以执行**vlan batch** { *vlan-id1 vlan-id2* }命令，创建多个不连续的VLAN，VLAN号之间需要有空格。

配置验证

```
[SWA]display vlan
The total number of vlans is : 4
--------------------------------------------------------------
U:Up; D:Down; TG:Tagged; UT:Untagged; MP:Vlan-mapping;
ST:Vlan-stacking; #: ProtocolTransparent-vlan; *:Management-
vlan;
----------------------------------------------------------------
VID  Type    Ports
----------------------------------------------------------------
1     common   UT:GE0/0/1(U) ......
2     common
3     common
10    common
......
```


Page 15

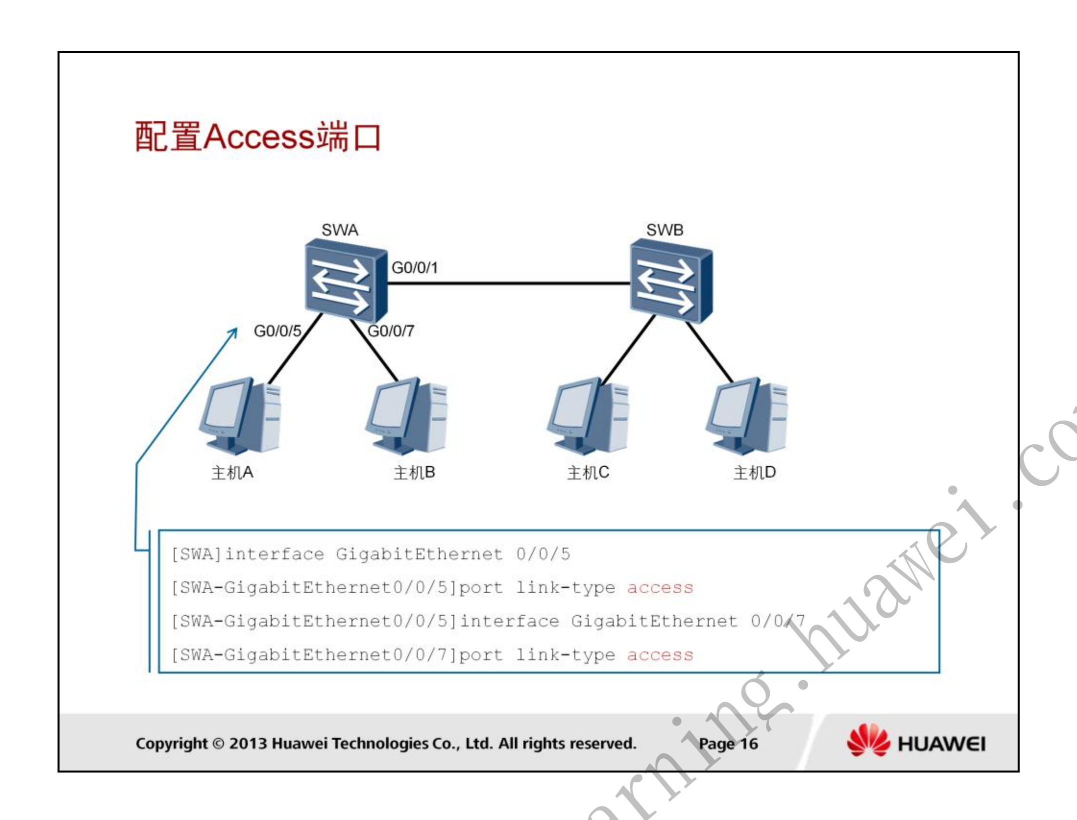


创建VLAN后，可以执行**display vlan**命令验证配置结果。如果不指定任何参数，则该命令将显示所有VLAN的简要信息。

执行**display vlan** [*vlan-id* [**verbose**]]命令，可以查看指定VLAN的详细信息，包括VLAN ID、类型、描述、VLAN的状态、VLAN中的端口、以及VLAN中端口的模式等。

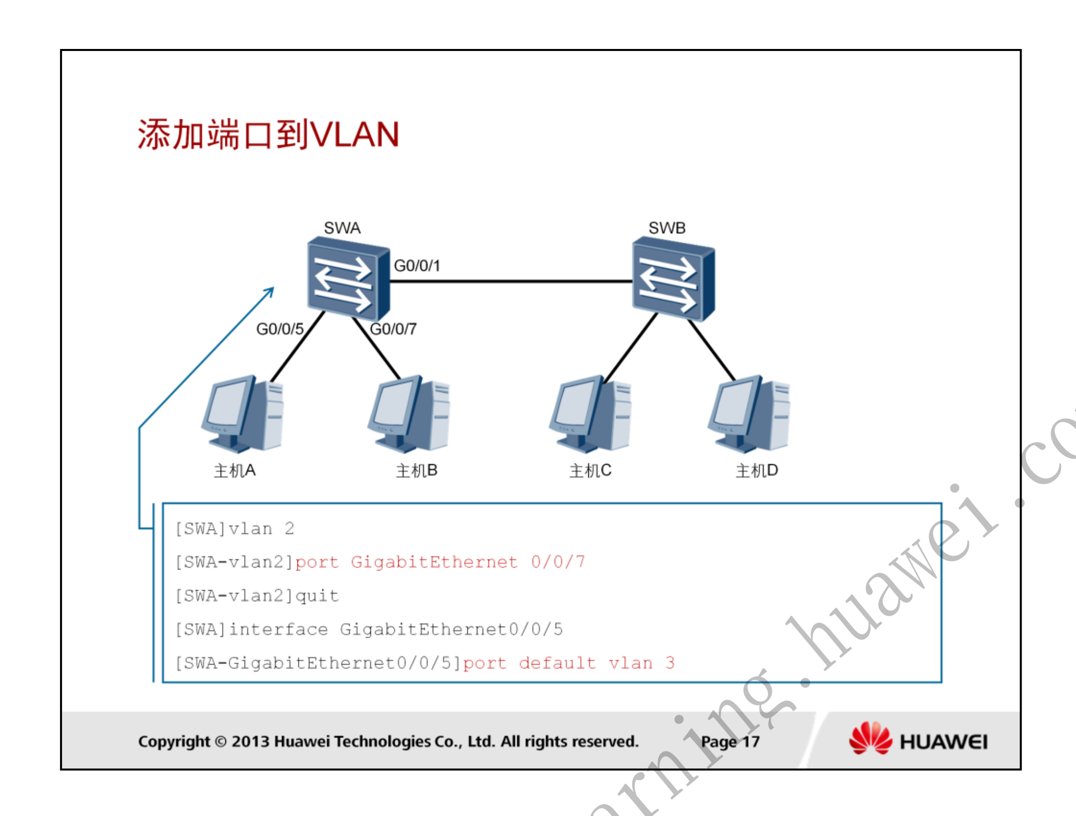
执行**display vlan** *vlan-id* **statistics**命令，可以查看指定VLAN中的流量统计信息。

执行**display vlan summary**命令，可以查看系统中所有VLAN的汇总信息。



华为X7系列交换机上，默认的端口类型是hybrid。

配置端口类型的命令是**port link-type** <*type*>，*type*可以配置为Access，Trunk或Hybrid。需要注意的是，如果查看端口配置时没有发现端口类型信息，说明端口使用了默认的hybrid端口链路类型。当修改端口类型时，必须先恢复端口的默认VLAN配置，使端口属于缺省的VLAN 1。



可以使用两种方法把端口加入到VLAN。

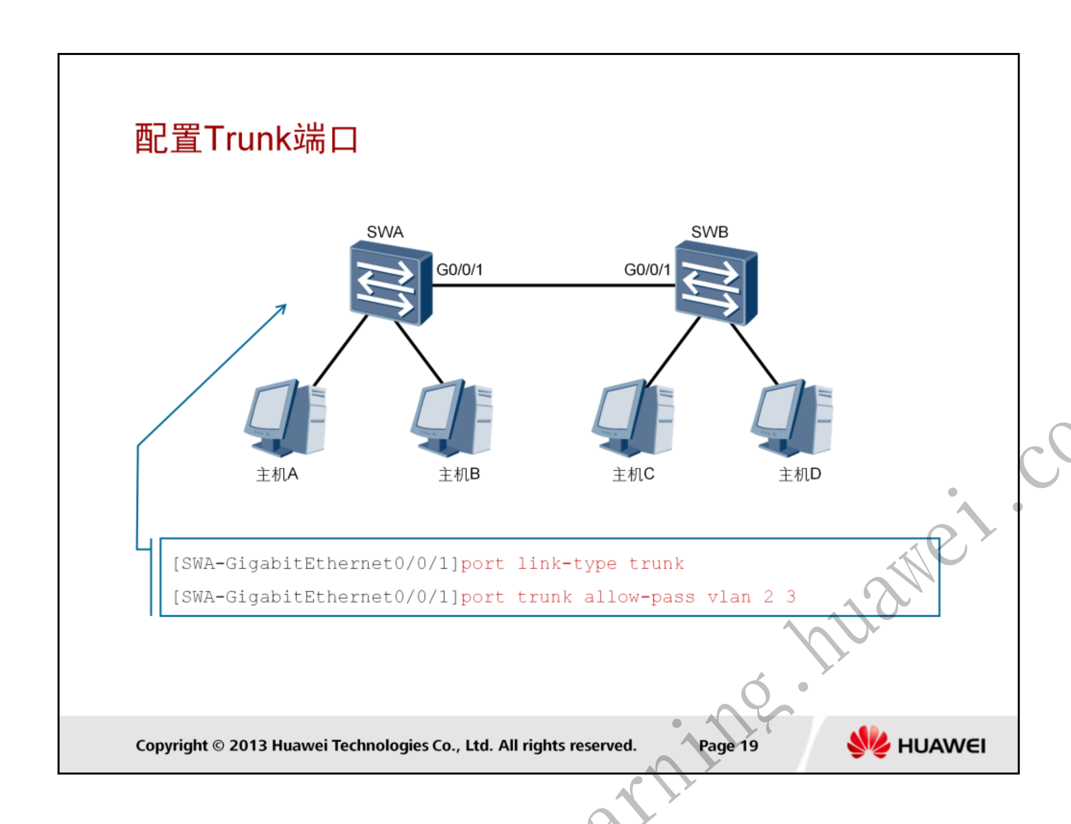
1. 第一种方法是进入到VLAN视图，执行port <interface>命令，把端口加入VLAN。
2. 第二种方法是进入到接口视图，执行port default <vlan-id>命令，把端口加入VLAN。vlan-id是指端口要加入的VLAN。

配置验证

```
[SWA]display vlan
The total number of vlans is : 4
------------------------------------------------------------
U:Up; D:Down; TG:Tagged; UT:Untagged; MP:Vlan-mapping;
ST:Vlan-stacking; #: ProtocolTransparent-vlan; *:Management-
vlan;
--------------------------------------------------------------
VID  Type     Ports
--------------------------------------------------------------
1     common   UT:GE0/0/1(U) ……
2     common   UT:GE0/0/7(U)
3     common   UT:GE0/0/5(U)
10    common
……
```


HUAWEI

执行**display vlan**命令，可以确认端口是否已经加入到VLAN中。在本示例中，端口GigabitEthernet0/0/5和GigabitEthernet0/0/7分别加入了VLAN 3和VLAN 2。**UT**表明该端口发送数据帧时，会剥离VLAN标签，即此端口是一个Access端口或不带标签的Hybrid端口。**U**或**D**分别表示链路当前是Up状态或Down状态。



配置Trunk时，应先使用**port link-type trunk**命令修改端口的类型为Trunk，然后再配置Trunk端口允许哪些VLAN的数据帧通过。执行**port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }命令，可以配置端口允许的VLAN，all表示允许所有VLAN的数据帧通过。

执行**port trunk pvid vlan** *vlan-id*命令，可以修改Trunk端口的PVID。修改Trunk端口的PVID之后，需要注意：缺省VLAN不一定是端口允许通过的VLAN。只有使用命令**port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }允许缺省VLAN数据通过，才能转发缺省VLAN的数据帧。交换机的所有端口默认允许VLAN1的数据通过。

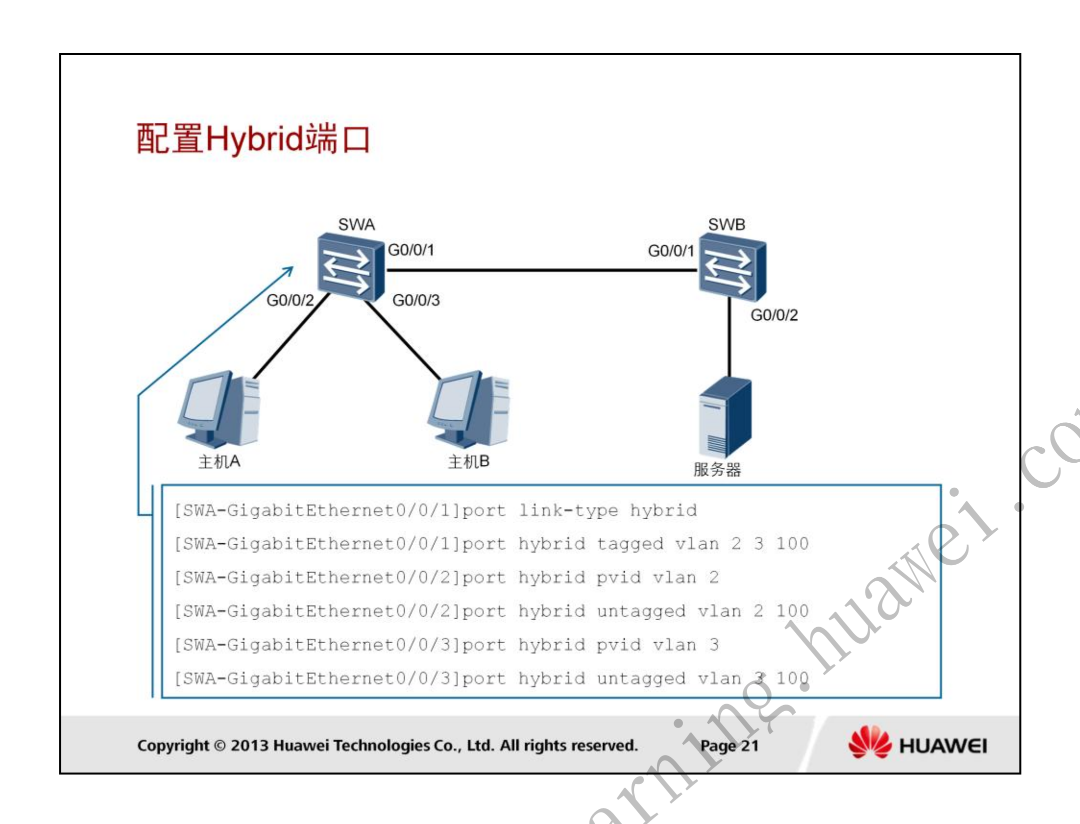
在本示例中，将SWA的G0/0/1端口配置为Trunk端口，该端口PVID默认为1。配置**port trunk allow-pass vlan** 2 3命令之后，该Trunk允许VLAN 2和VLAN 3的数据流量通过。

配置验证

```
[SWA]display vlan
The total number of vlans is : 4
------------------------------------------------------------
U:Up; D:Down; TG:Tagged; UT:Untagged; MP:Vlan-mapping;
ST:Vlan-stacking; #: ProtocolTransparent-vlan; *:Management-
vlan;
--------------------------------------------------------------
VID  Type    Ports
--------------------------------------------------------------
1     common  UT:GE0/0/1(U) ……
2     common  UT:GE0/0/7(D) TG:GE0/0/1(U)
3     common  UT:GE0/0/5(U) TG:GE0/0/1(U)
10    common
……
```




执行**display vlan**命令可以查看修改后的配置。TG表明该端口在转发对应VLAN的数据帧时，不会剥离标签，直接进行转发，该端口可以是Trunk端口或带标签的Hybrid端口。本示例中，GigabitEthernet0/0/1在转发VLAN 2和VLAN3的流量时，不剥离标签，直接转发。



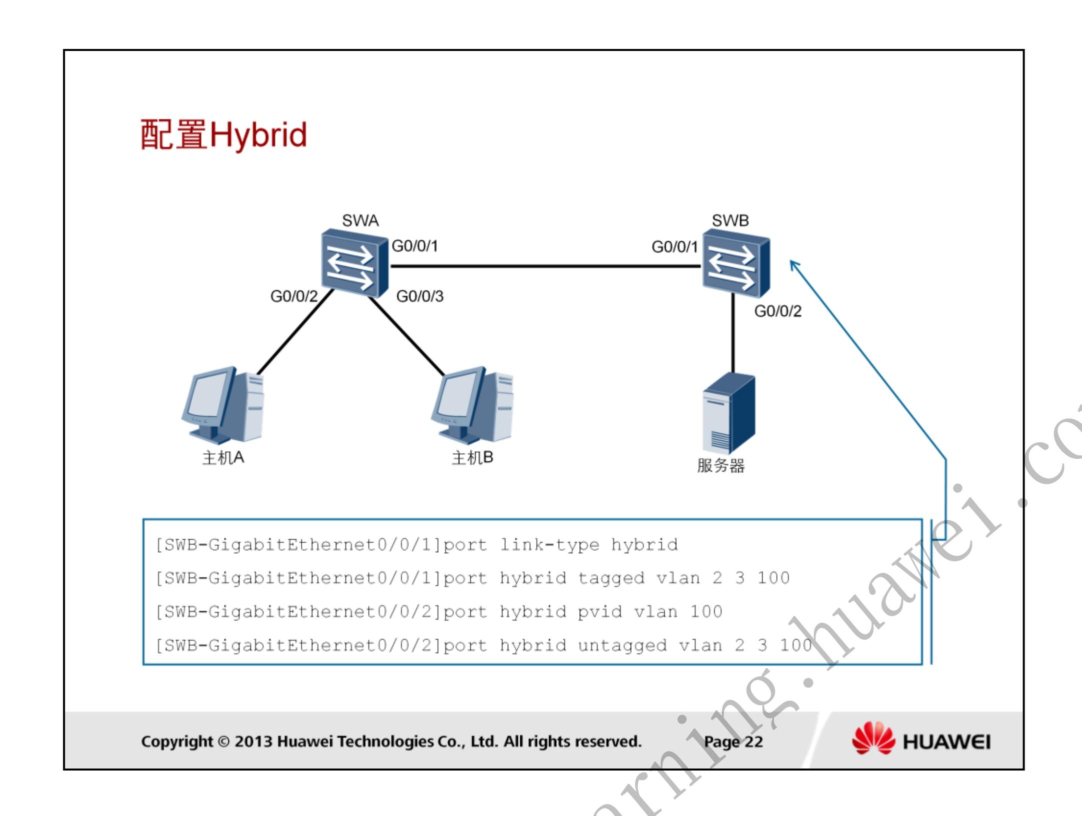
port link-type hybrid命令的作用是将端口的类型配置为Hybrid。默认情况下，X7系列交换机的端口类型是Hybrid。因此，只有在把Access口或Trunk口配置成Hybrid时，才需要执行此命令。

port hybrid tagged vlan{ { *vlan-id1* [**to** *vlan-id2*] } | **all** }命令用来配置允许哪些VLAN的数据帧以Tagged方式通过该端口。

port hybrid untagged vlan { { *vlan-id1* [**to** *vlan-id2*] } | **all** }命令用来配置允许哪些VLAN的数据帧以Untagged方式通过该端口。

在本示例中，要求主机A和主机B都能访问服务器，但是它们之间不能互相访问。此时通过命令port link-type hybrid配置交换机连接主机和服务器的端口，以及交换机互连的端口都为Hybrid类型。通过命令port hybrid pvid vlan 2配置交换机连接主机A的端口的PVID是2。类似地，连接主机B的端口的PVID是3，连接服务器的端口的PVID是100。

通过在G0/0/1端口下使用命令port hybrid tagged vlan 2 3 100，配置VLAN2,VLAN3和VLAN100的数据帧在通过该端口时都携带标签。在G0/0/2端口下使用命令port hybrid untagged vlan 2 100，配置VLAN2和VLAN100的数据帧在通过该端口时都不携带标签。在G0/0/3端口下使用命令port hybrid untagged vlan 3 100，配置VLAN3和VLAN100的数据帧在通过该端口时都不携带标签。



在SWB上继续进行配置，在G0/0/1端口下使用命令**port link-type hybrid**配置端口类型为Hybrid。

在G0/0/1端口下使用命令**port hybrid tagged vlan** 2 3 100，配置VLAN2，VLAN3和VLAN100的数据帧在通过该端口时都携带标签。

在G0/0/2端口下使用命令**port hybrid untagged vlan** 2 3 100，配置VLAN2，VLAN3和VLAN100的数据帧在通过该端口时都不携带标签。

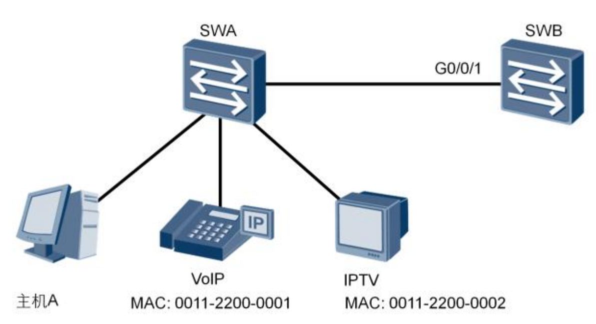
配置验证

```
[SWA]display vlan
The total number of vlans is : 4
------------------------------------------------------------
U:Up; D:Down; TG:Tagged; UT:Untagged; MP:Vlan-mapping; ST:Vlan-
stacking; #: ProtocolTransparent-vlan; *:Management-vlan;
1    common    UT:GE0/0/1(U)……
2    common    UT:GE0/0/2(U)
               TG:GE0/0/1(U)
3    common    UT:GE0/0/3(U)
               TG:GE0/0/1(U)
100   common   UT:GE0/0/2(U)       GE0/0/3(U)
               TG:GE0/0/1(U)
```




在SWA上执行**display vlan**命令，可以查看hybrid端口的配置。在本示例中，GigabitEthernet 0/0/2在发送VLAN2和VLAN100的数据帧时会剥离标签。GigabitEthernet 0/0/3在发送VLAN3和VLAN100的数据帧时会剥离标签。GigabitEthernet 0/0/1允许VLAN 2，VLAN 3和VLAN 100的带标签的数据帧通过。此配置满足了多个VLAN可以访问特定VLAN，而其他VLAN间不允许互相访问的需求。

Voice VLAN应用



- 通过配置Voice VLAN可以区分语音流量和业务流量，使语音流量优于业务流量，从而为语音流量提供服务保证。

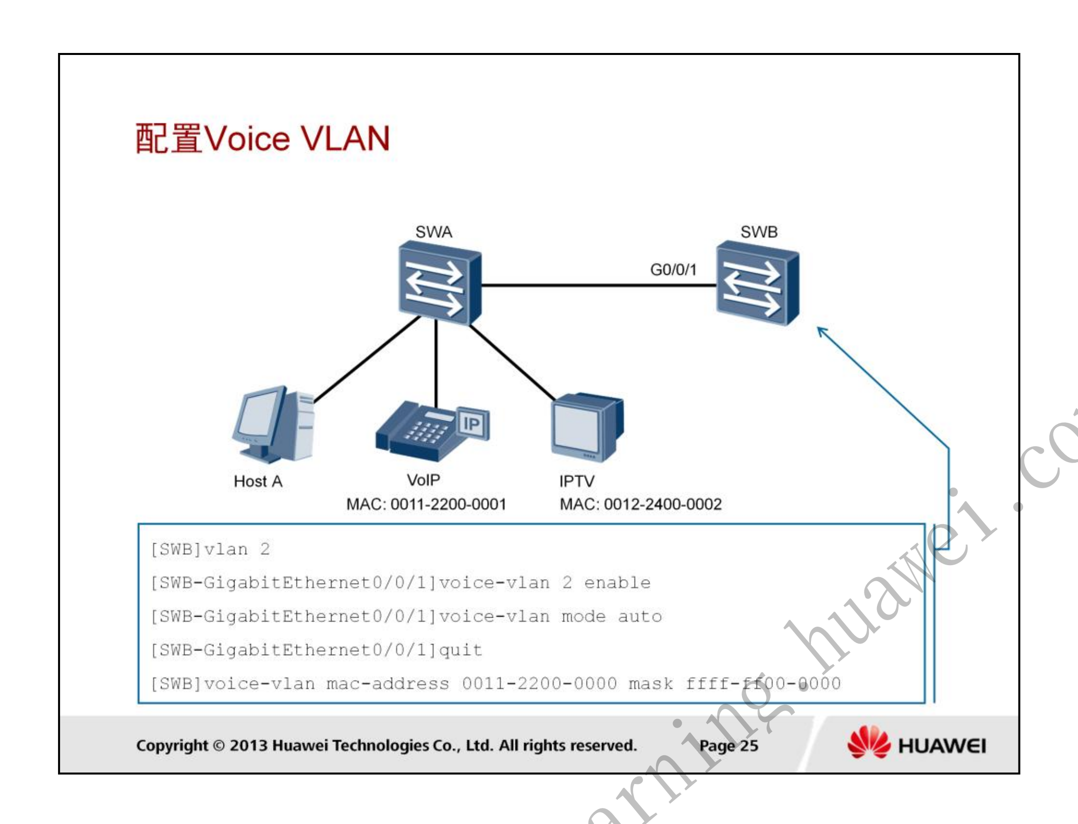
 Page 24



随着IP网络的融合，TCP/IP网络可以为高速上网HSI（High Speed Internet）业务、VoIP（Voice over IP）业务、IPTV（Internet Protocol Television）业务提供服务。

语音数据在传输时需要具有比其他业务数据更高的优先级，以减少传输过程中可能产生的时延和丢包现象。

为了区分语音数据流，可在交换机上部署Voice VLAN功能，把VoIP的电话流量进行VLAN隔离，并配置更高的优先级，从而能够保证通话质量。



执行**voice-vlan** <*vlan-id*> **enable**命令，可以把VLAN 2到VLAN 4094之间的任一VLAN配置成语音VLAN。

执行**voice-vlan mode** <*mode*>命令，可以配置端口加入语音VLAN的模式。

端口加入Voice VLAN的模式有两种：

1. 自动模式：使能Voice VLAN功能的端口根据进入端口的数据流中的源MAC地址字段来判断该数据流是否为语音数据流。源MAC地址符合系统设置的语音设备OUI（Organizationally Unique Identifier）地址的报文认为是语音数据流。接收到语音数据流的端口将自动加入Voice VLAN中传输，并通过老化机制维护Voice VLAN内的端口数量。
2. 手动模式：当接口使能Voice VLAN功能后，必须通过手工将连接语音设备的端口加入或退出Voice VLAN中，这样才能保证Voice VLAN功能生效。

执行 **voice-vlan mac-address** *mac-address* **mask** *oui-mask* [**description** *text*]命令，用来配置Voice VLAN的OUI地址。OUI地址表示一个MAC地址段。交换机将48位的MAC地址和掩码的对应位做“与”运算可以确定出OUI地址。接入设备的MAC地址和OUI地址匹配的位数，由掩码中全“1”的长度决定。例如，MAC地址为0001–0001–0001，掩码为FFFF-FF00–0000，那么将MAC地址与其相应掩码位执行“与”运算的结果就是OUI地址0001–0000–0000。只要接入设备的MAC地址前24位和OUI地址的前24位匹配，那么使能Voice VLAN功能的端口将认为此数据流是语音数据流，接入的设备是语音设备。

配置验证

```
[SWB]display voice-vlan status
Voice VLAN Configurations:
-----------------------------------------------------------
Voice VLAN ID              : 2
Voice VLAN status          : Enable
Voice VLAN aging time      : 1440(minutes)
Voice VLAN 8021p remark    : 6
Voice VLAN dscp remark     : 46
-----------------------------------------------------------
Port Information:
-----------------------------------------------------------
Port                      Add-Mode   Security-Mode   Legacy
-----------------------------------------------------------
GigabitEthernet0/0/1      Auto       Security        Disable
```




执行**display voice-vlan status**命令，可以查看语音VLAN的信息，包括状态、工作模式、老化时间、以及使能了语音VLAN功能的端口信息。

Add-Mode字段表明语音VLAN的添加模式。自动模式中，使能了语音VLAN功能后，端口可以自动加入到语音VLAN。如果语音设备发送的报文的MAC地址匹配了OUI，连接该语音设备的端口也会加入语音VLAN。如果在老化时间内，端口没有收到语音设备的任何语音数据报文，端口自动会被删除。手动模式中，在端口上使能了语音VLAN功能之后，必须手动把端口添加到语音VLAN中。

Security-Mode字段表示Voice VLAN端口的工作模式，有两种：

1. 正常模式：可以传输语音数据和业务数据，但是容易受到恶意数据流量的攻击。
2. 安全模式：只允许传输语音数据流。安全模式可以防止Voice VLAN受到恶意数据流量的攻击，但是检查报文的工作会占用一定的系统资源。

Legacy字段表明端口是否开启与其他厂商语音设备互通的功能，Enable表示开启，Disable表示关闭。



总结

- 如果一个Trunk链路PVID是5，且端口下配置port trunk allow-pass vlan 2 3，那么哪些VLAN的流量可以通过该Trunk链路进行传输?
- PVID为2的Access端口收到一个不带标记的帧会采取什么样的动作?



1. 执行了**port trunk allow-pass vlan 2 3**命令后，VLAN 5的数据帧不能在此链路上进行传输。VLAN 1的数据默认也可以通过Trunk链路进行传输。所以VLAN 1，VLAN 2和VLAN 3的数据帧可以在Trunk链路上传输。
2. 收到不带标签的数据帧后，PVID为2的Access端口会给数据帧打上VLAN 2的标签。然后交换机会根据标签和目的MAC地址将数据帧发送到其他端口。


谢谢
www.huawei.com


GARP&GVRP
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

GARP（Generic Attribute Registration Protocol），全称是通用属性注册协议，它为处于同一个交换网内的交换机之间提供了一种分发、传播、注册某种信息（VLAN属性、组播地址等）的手段。

GVRP是GARP的一种具体应用或实现，主要用于维护设备动态VLAN属性。通过GVRP协议，一台交换机上的VLAN信息会迅速传播到整个交换网络。GVRP实现了LAN属性的动态分发、注册和传播，从而减少了网络管理员的工作量，也能保证VLAN配置的正确性。



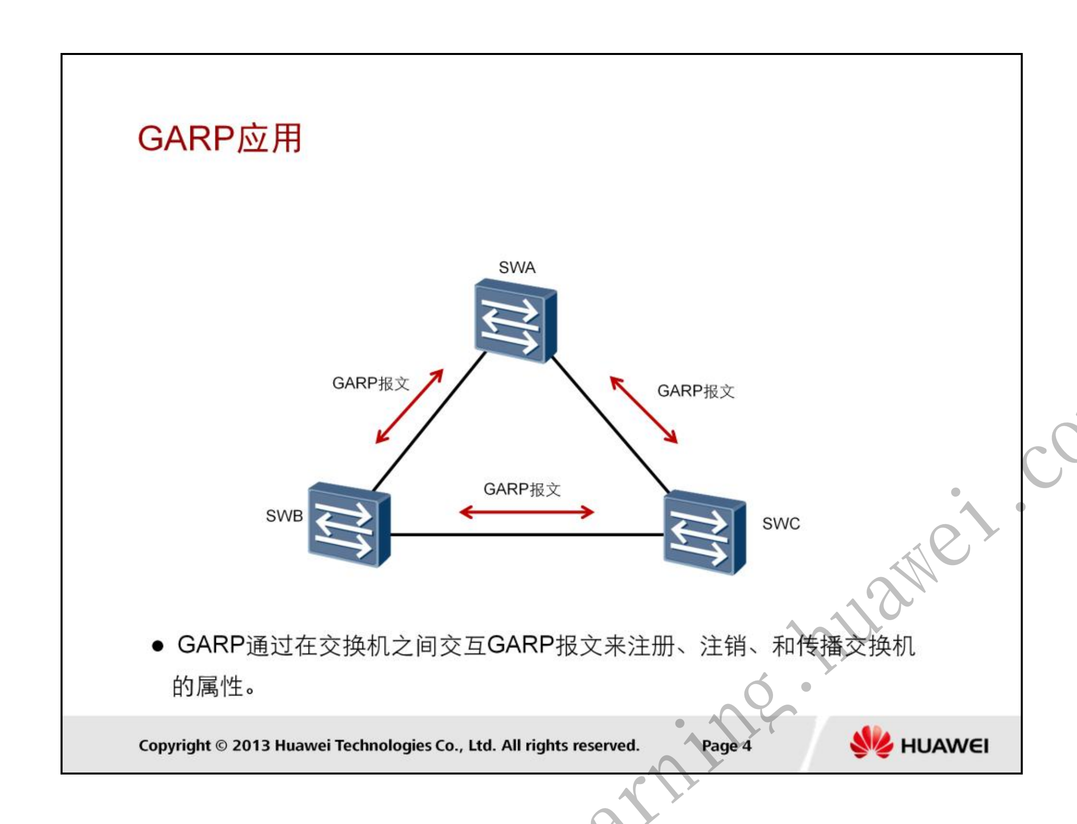


学习目标

学完本课程后，您应该能：

- 掌握GVRP的工作原理
- 掌握GVRP的基本配置

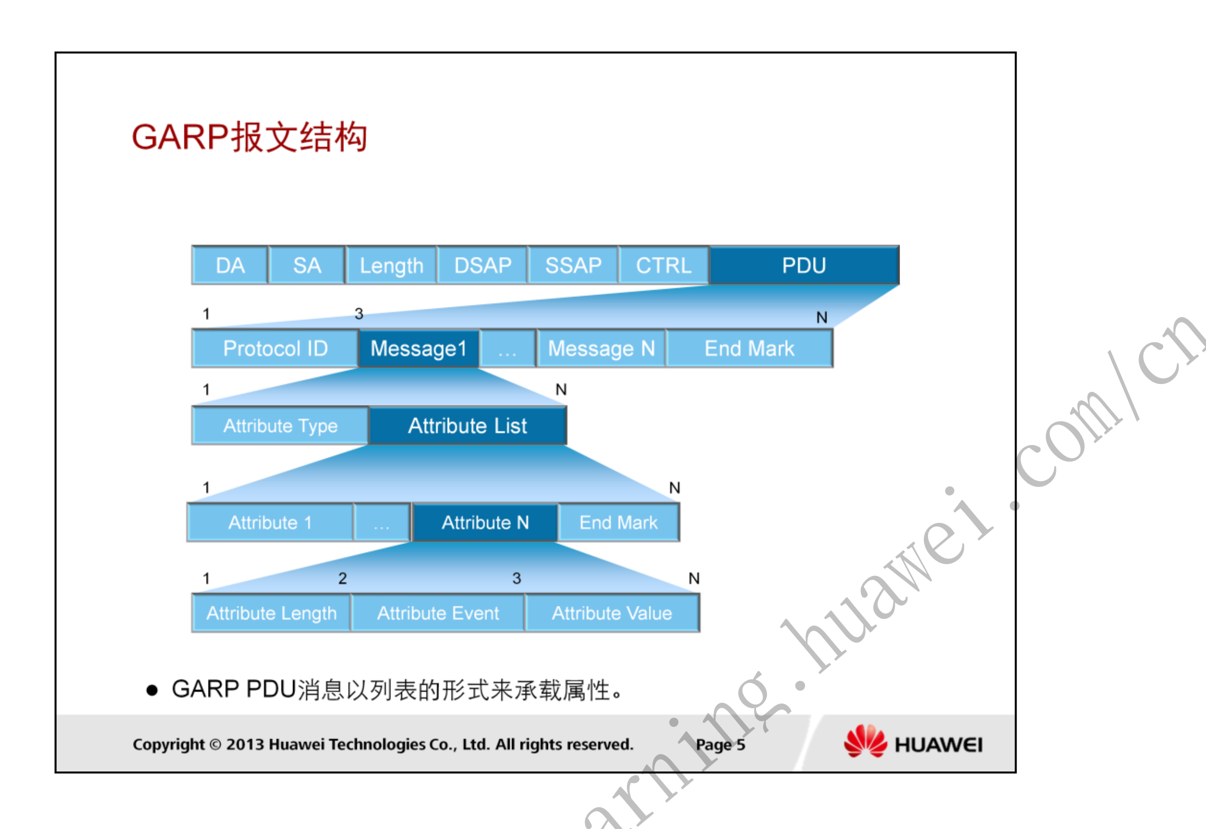




GARP（Generic Attribute Registration Protocol），全称是通用属性注册协议。它为处于同一个交换网内的交换成员之间提供了一种分发、传播、注册某种信息的手段，这些信息可以是VLAN信息、组播组地址等。通过GARP机制，一个GARP成员上的配置信息会迅速传播到整个交换网。

GARP主要用于大中型网络中，用来提升交换机的管理效率。在大中型网络中，如果管理员手动配置和维护每台交换机，将会带来巨大的工作量。使用GARP可以自动完成大量交换机的配置和部署，减少了大量的人力消耗。

GARP本身仅仅是一种协议规范，并不作为一个实体在交换机中存在。遵循GARP协议的应用实体称为GARP应用，目前主要的GARP应用为GVRP和GMRP。



GARP协议报文采用IEEE 802.3 Ethernet封装形式，目的MAC地址为多播MAC地址01-80-C2-00-00-21。GARP使用PDU包含的消息定义属性，根据属性类型字段和属性列表识别消息。属性列表中包含多个属性。每个属性包含属性长度、属性事件和属性值字段。属性长度范围在2到255个字节之间。属性值为属性定义了具体的值。属性事件是0到5之间的一个值，这些值代表GARP支持的不同事件类型，具体含义如下：

0：代表LeaveAll事件；

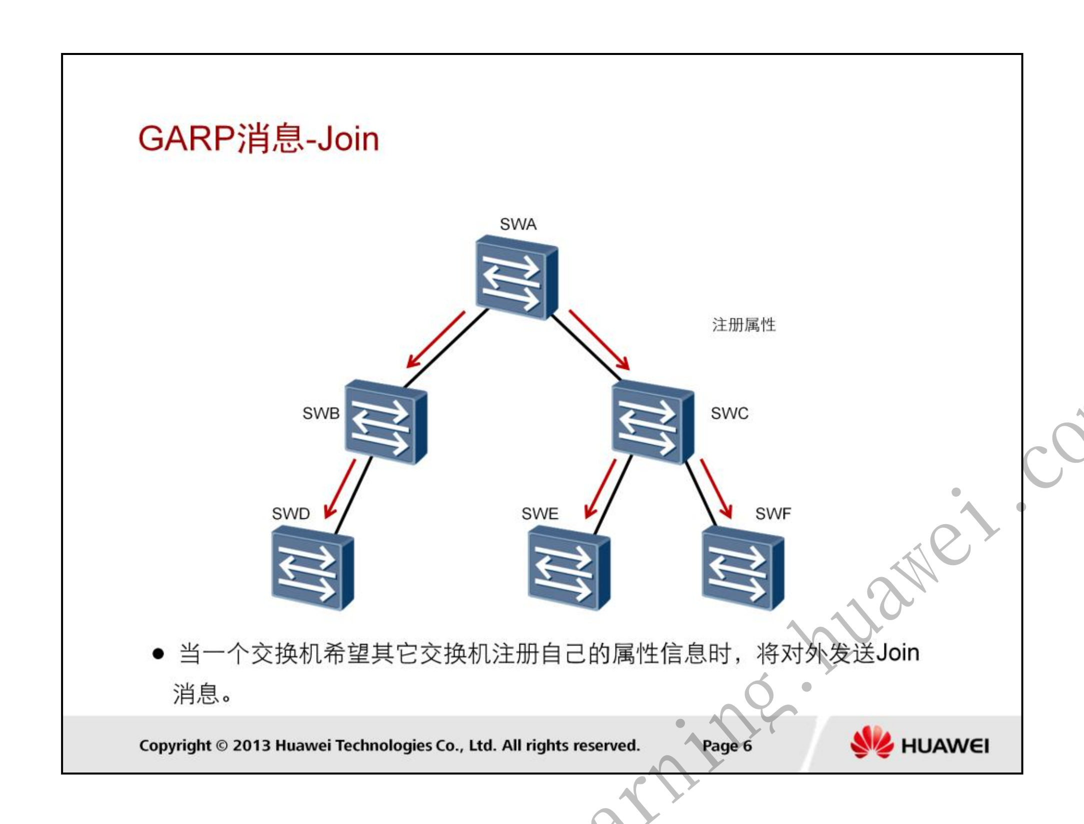
1：代表JoinEmpty事件；

2：代表JoinIn事件；

3：代表LeaveEmpty事件；

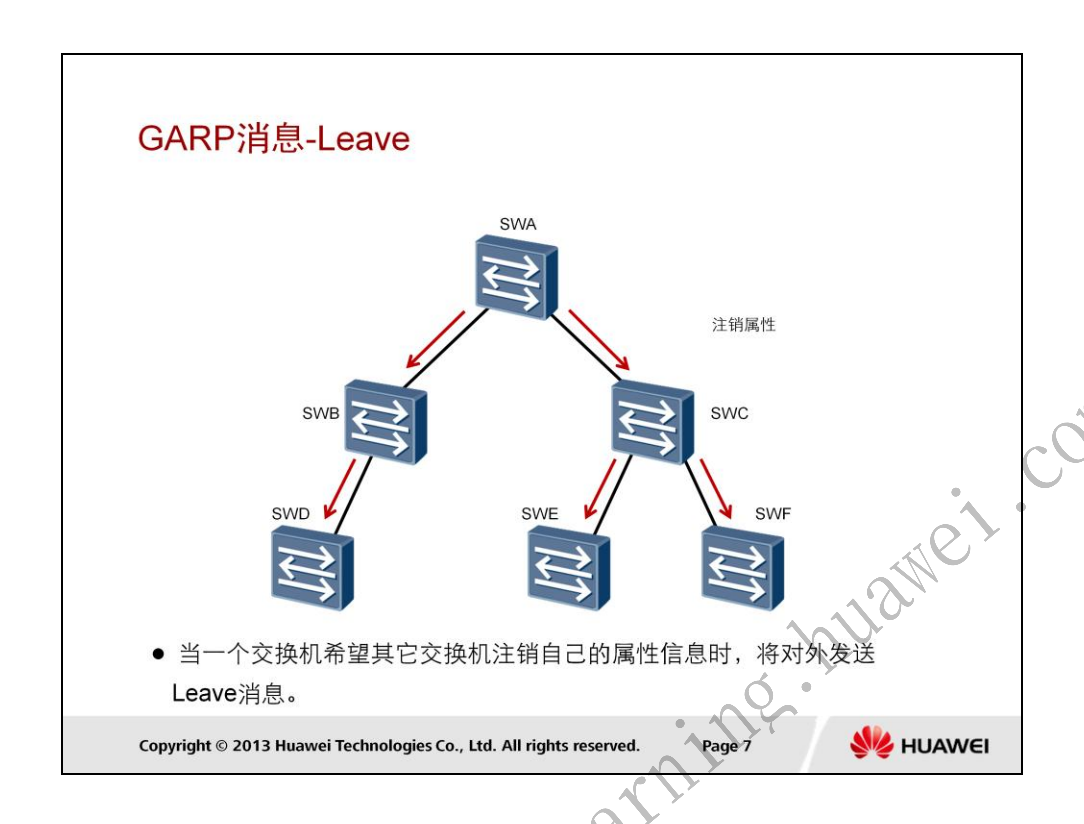
4：代表LeaveIn事件；

5：代表Empty事件。



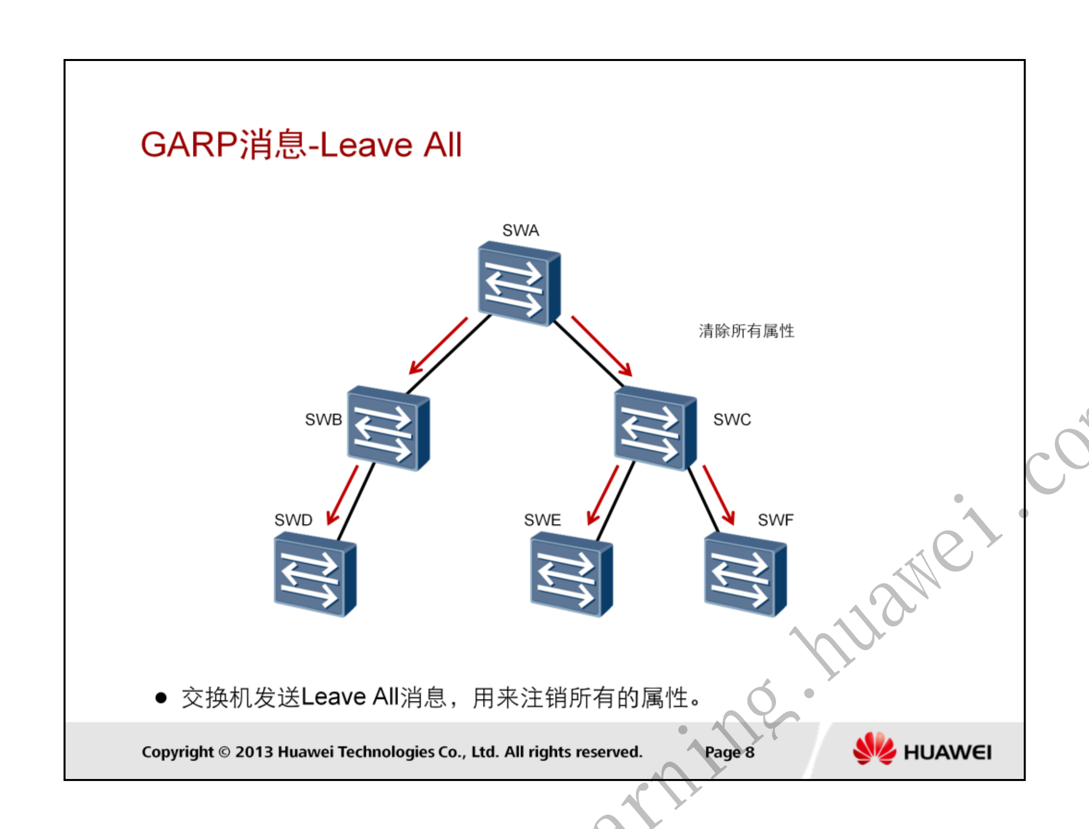
如果GARP参与者希望其他交换机注册自己的属性，则会向它们发送Join消息。

如果一个GARP参与者收到其他交换机发送的Join消息，或者手动配置了某些属性，该参与者也会向其他交换机发送Join消息，让其他交换机注册这些新的属性。

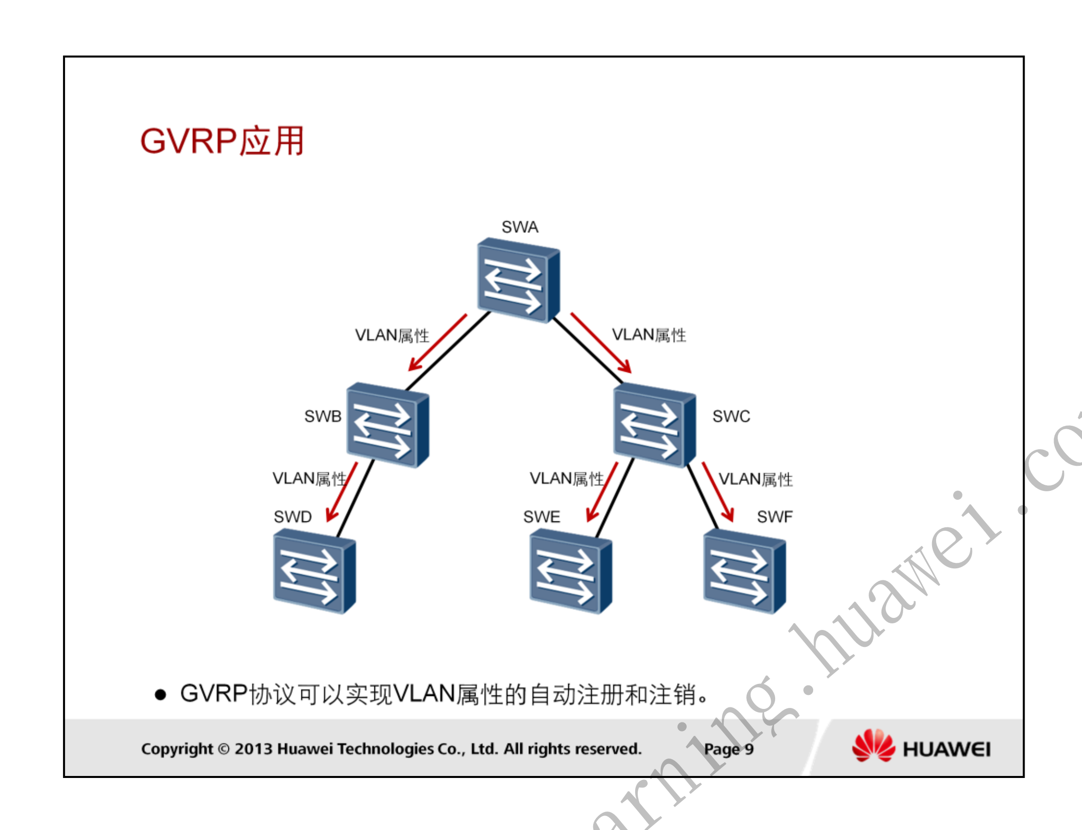


如果GARP参与者希望其他交换机注销自己的属性，则会向它们发送Leave消息。

如果GARP参与者收到其他交换机发送的Leave消息，或者手动注销了某些属性，该参与者也会向其他交换机发送Leave消息。



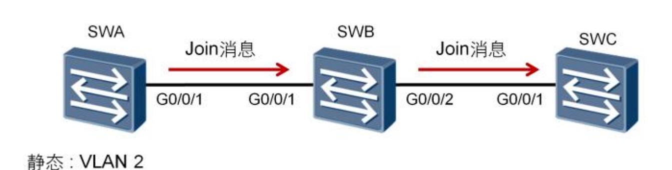
如果GARP参与者希望其他交换机注销所有属性，来重新注册自己发送的属性信息，则会向它们发送Leave All消息。



GVRP（GARP VLAN Registration Protocol），称为VLAN注册协议。GVRP基于GARP的工作机制，是GARP的一种应用。GVRP用来维护交换机中的VLAN动态注册信息，并传播该信息到其它的交换机中。支持GVRP特性的交换机能够接收来自其它交换机的VLAN注册信息，并动态更新本地的VLAN注册信息，包括当前的VLAN、VLAN成员等。支持GVRP特性的交换机能够将本地的VLAN注册信息向其它交换机传播，以便使同一交换网内所有支持GVRP特性的设备的VLAN信息达成一致。

交换机可以静态创建VLAN，也可以动态通过GVRP获取VLAN信息。手动配置的VLAN是静态VLAN，通过GVRP创建的VLAN是动态VLAN。GVRP传播的VLAN注册信息包括本地手工配置的静态注册信息和来自其它交换机的动态注册信息。

GVRP单向注册



- 在SWA上创建静态VLAN2，通过VLAN属性的单向注册，SWB和SWC会学习到动态VLAN2，并将相应端口自动加入到VLAN2中。
- SWB的G0/0/2端口没有收到Join消息，不会被加入到VLAN2中。

 Page 10

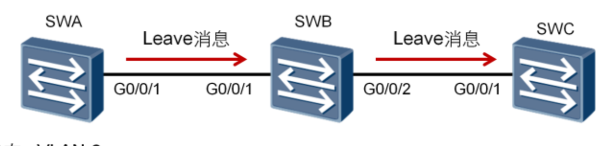


如图所示，所有交换机以及互连的接口都已经启用GVRP协议，各交换机之间相连的端口均为Trunk端口并配置为允许所有VLAN的数据通过。

在SWA上手动创建VLAN2之后，SWA的G0/0/1端口会注册此VLAN并发送声明给SWB，SWB的G0/0/1端口接收到由SWA发来的声明后，会在此端口注册VLAN2，然后从G0/0/2发送声明给SWC，SWC的G0/0/1收到声明后也会注册VLAN2。通过此过程就完成了VLAN2从SWA向其他交换机的单向注册。只有注册了VLAN2的端口才可以接收和转发VLAN2的数据，没有注册VLAN2的端口会丢弃VLAN2的数据，如SWB的G0/0/2端口没有收到VLAN2的Join消息，不会注册VLAN2，就不能接收和转发VLAN2的数据。

为使VLAN 2流量可以双向互通，还需要进行SWC到SWA方向的VLAN属性的注册过程。

GVRP单向注销



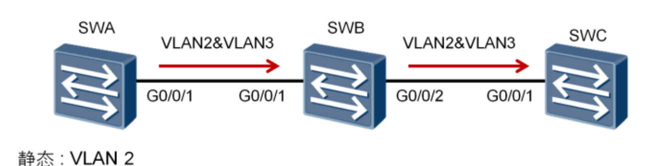
- 当交换机不再需要VLAN2时，可以通过VLAN属性的注销过程将VLAN2删除。

 Page 11 

如图所示，如果所有交换机都不再需要VLAN2，可以在SWA上手动删除VLAN2，则GVRP会通过发送Leave消息，注销SWB和SWC上G0/0/1端口的VLAN2信息。

为了彻底删除所有设备上的VLAN 2，需要进行VLAN属性的双向注销。

注册模式-Normal



- 交换机端口默认为Normal模式，允许静态和动态VLAN注册，同时会发送静态VLAN和动态VLAN的声明消息。

 Page 12

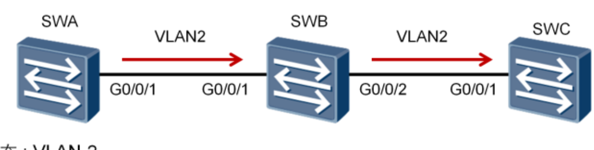


GVRP的注册模式包括：Normal、Fixed和Forbidden。

当一个Trunk端口被配置为Normal注册模式时，允许在该端口动态或手工创建、注册和注销VLAN，同时会发送静态VLAN和动态VLAN的声明消息。X7系列交换机在运行GVRP协议时，端口的注册模式都默认为Normal。

本例中，在SWA上存在手动创建的VLAN2和动态学习的VLAN3的信息，三台交换机的注册模式都默认为Normal，则SWA发送的Join消息中会包含VLAN2和VLAN3的信息，SWB的G0/0/1端口会注册VLAN2和VLAN3，之后会同样发送Join消息给SWC，SWC的G0/0/1端口也会注册VLAN2和VLAN3。

注册模式-Fixed



静态：VLAN 2
动态：VLAN 3

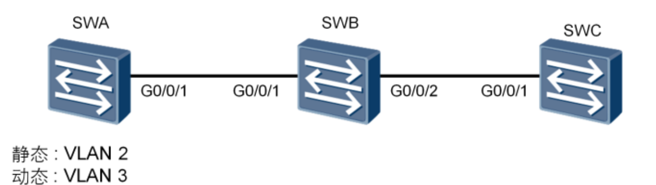
- SWA的G0/0/1端口为Fixed模式，不允许动态VLAN在端口上注册或者注销，且只发送静态VLAN的声明消息。



Fixed注册模式中，GVRP不能动态注册或注销VLAN，只能发送静态VLAN注册信息。如果一个Trunk端口的注册模式被设置为Fixed模式，即使接口被配置为允许所有VLAN的数据通过，该接口也只允许手动配置的VLAN内的数据通过。

本例中，在SWA上存在手动创建的VLAN2和动态学习的VLAN3的信息，SWA的G0/0/1端口的注册模式被修改为Fixed，则SWA发送的Join消息中会只包含静态VLAN2的信息，SWB的G0/0/1端口会注册VLAN2。

注册模式-Forbidden



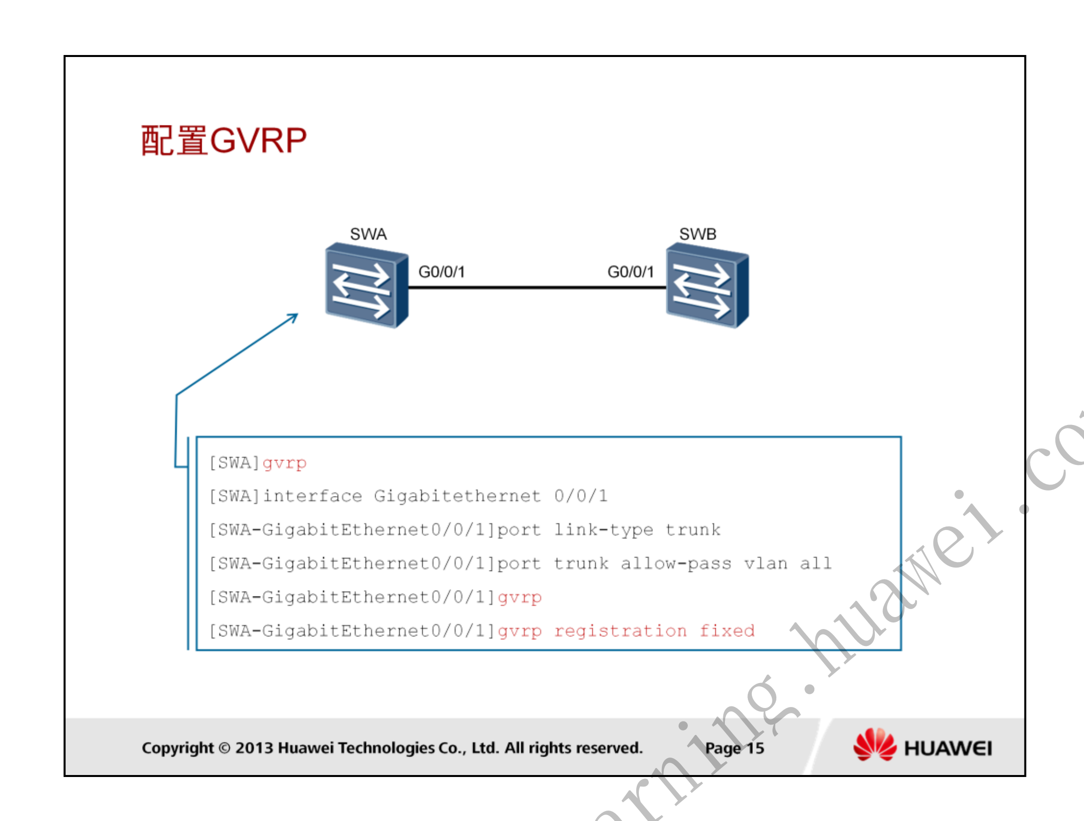
静态 : VLAN 2
动态 : VLAN 3

- SWA的G0/0/1端口为Forbidden模式，不允许动态VLAN在端口上进行注册，同时删除端口上除VLAN1外的所有VLAN。



Forbidden注册模式中，GVRP接口不能动态注册或注销VLAN，只保留VLAN1的信息。如果一个Trunk端口的注册模式被设置为Forbidden模式，即使端口被配置为允许所有VLAN的数据通过，该端口也只允许VLAN1的数据通过。

本例中，在SWA上存在手动创建的VLAN2和动态学习的VLAN3的信息，SWA的G0/0/1端口配置为Forbidden模式，不会发送VLAN2和VLAN3的信息，且只允许VLAN1的数据通过。



配置GVRP时必须先在系统视图下使能GVRP，然后在接口视图下使能GVRP。

在全局视图下执行**gvrp**命令，全局使能GVRP功能。

在接口视图下执行**gvrp**命令，在端口上使能GVRP功能。

执行**gvrp registration** *<mode>*命令，配置端口的注册模式，可以配置为Normal、Fixed和Forbidden。默认情况下，接口的注册模式为Normal模式。

配置验证

```
[SWA]display gvrp status
 GVRP is enabled
[SWA]display gvrp statistics
  GVRP statistics on port GigabitEthernet0/0/1
    GVRP status                              : Enabled
    GVRP registrations failed                : 0
    GVRP last PDU origin                     : 0000-0000-0000
    GVRP registration type                   : Fixed
```




执行**display gvrp status**命令，验证GVRP的配置，可以查看交换机是否使能了GVRP。

执行**display gvrp statistics**命令，可以查看GVRP中活动接口的信息。在本示例中，可以查看接口当前的GVRP状态为Enabled，注册类型为Fixed。



总结

- GVRP默认的注册模式是什么?
- 交换机使用GVRP传输VLAN信息时，需要哪些前提条件?

Page 17



1. 默认注册模式是Normal。
2. 配置了GVRP的交换机在传输VLAN信息时，需要首先配置链路两端的端口类型为Trunk，并且允许相应的VLAN数据通过。

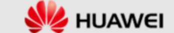

谢谢
www.huawei.com


VLAN间路由
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

部署了VLAN的传统交换机不能实现不同VLAN间的二层报文转发，因此必须引入路由技术来实现不同VLAN间的通信。VLAN路由可以通过二层交换机配合路由器来实现，也可以通过三层交换机来实现。



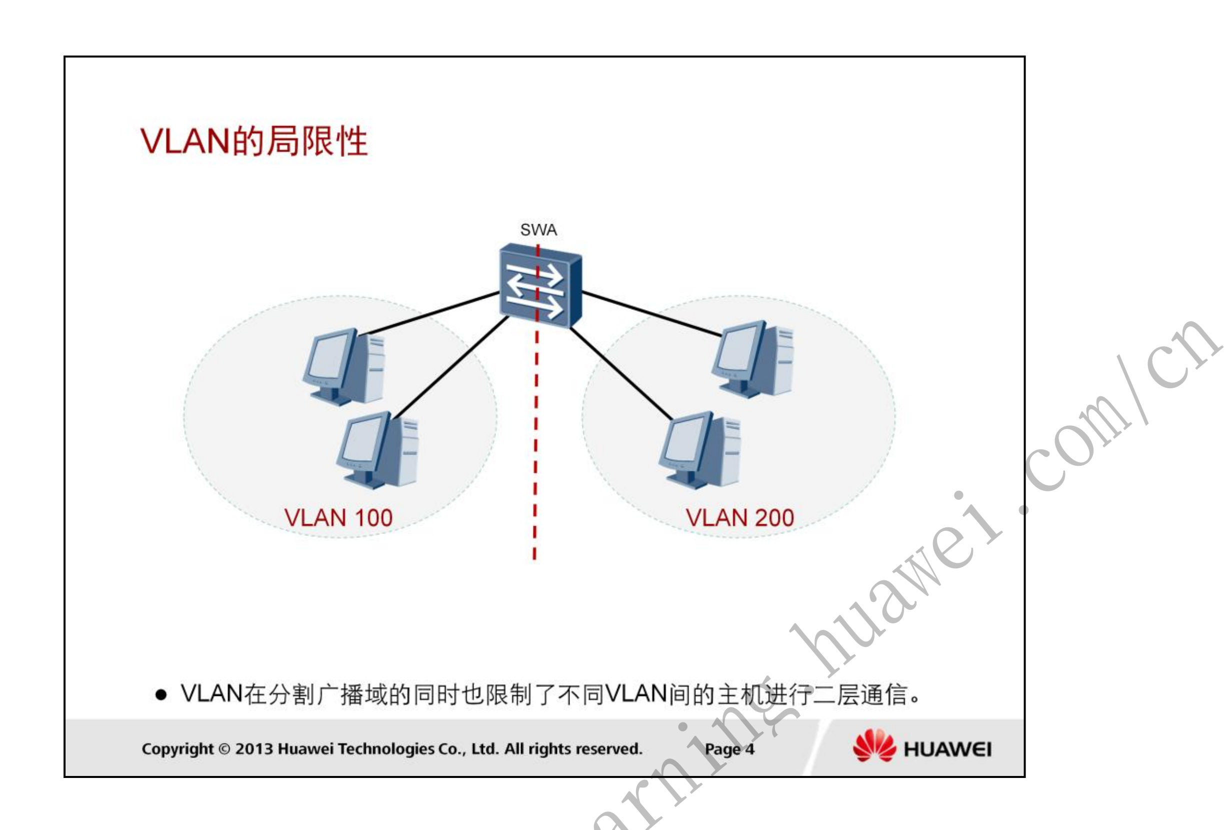


学习目标

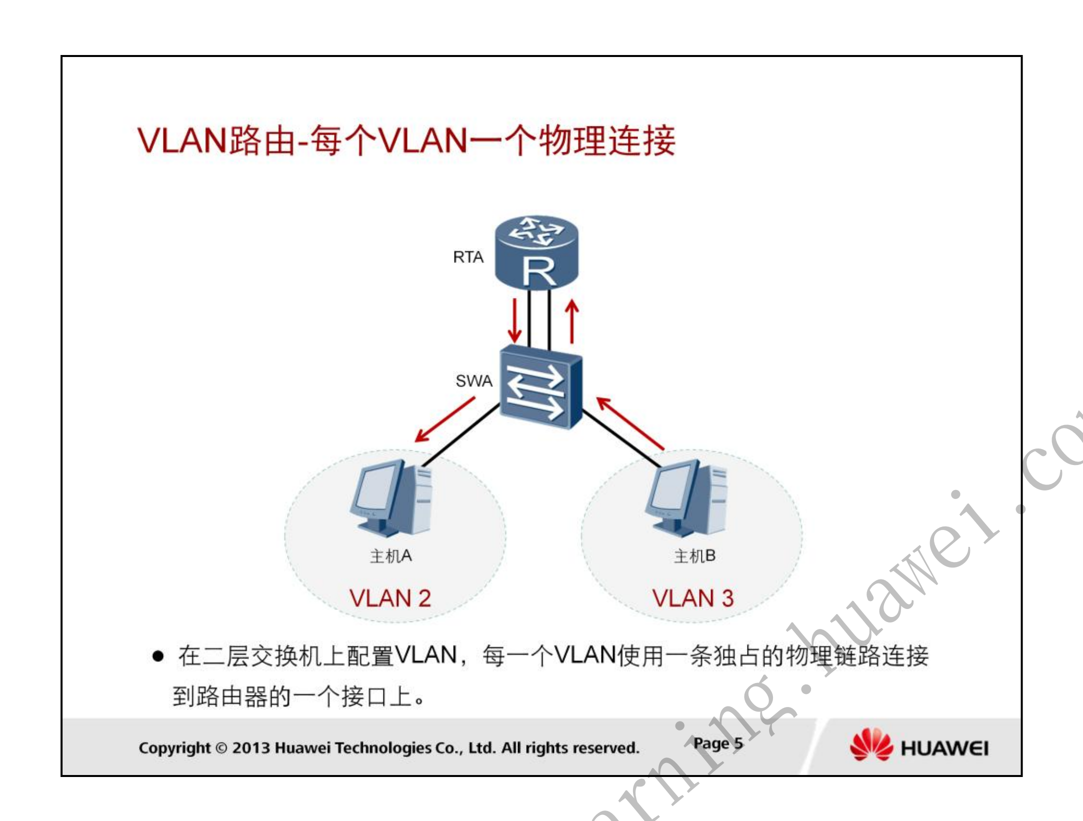
学完本课程后，您应该能：

- 掌握VLAN路由的应用场景
- 掌握VLAN路由的工作原理
- 掌握VLAN路由的基本配置





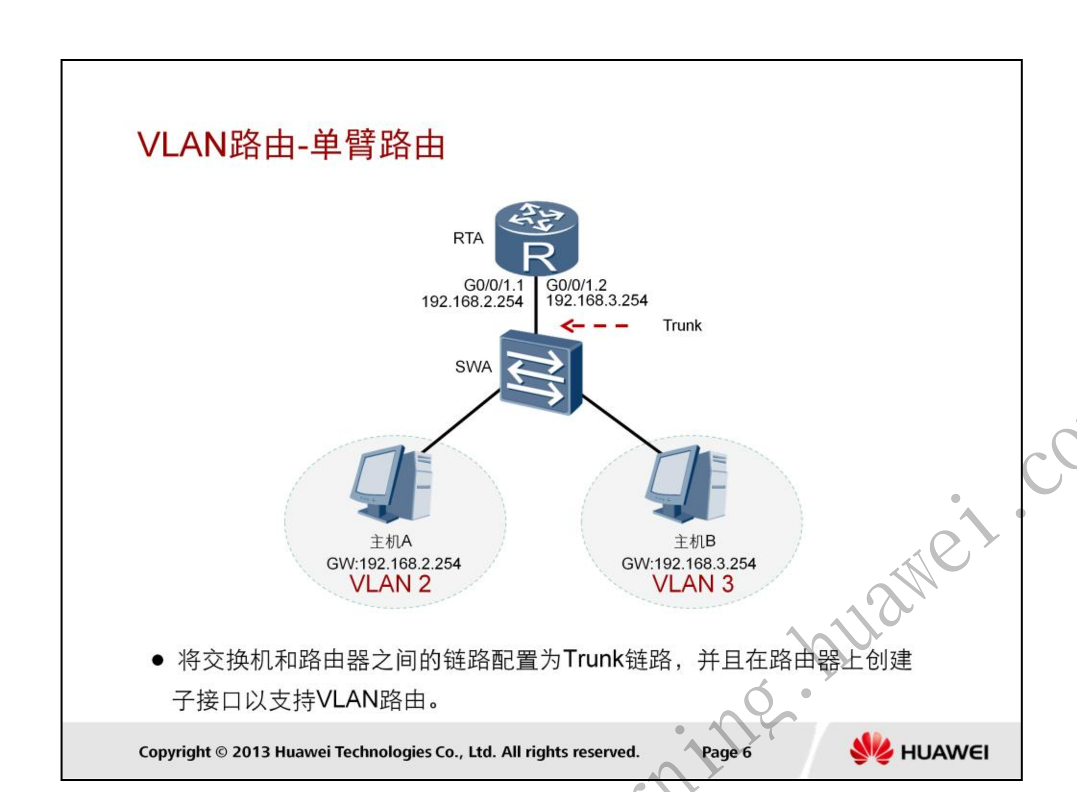
VLAN隔离了二层广播域，也严格地隔离了各个VLAN之间的任何二层流量，属于不同VLAN的用户之间不能进行二层通信。



因为不同VLAN之间的主机是无法实现二层通信的，所以必须通过三层路由才能将报文从一个VLAN转发到另外一个VLAN。

解决VLAN间通信问题的第一种方法是：在路由器上为每个VLAN分配一个单独的接口，并使用一条物理链路连接到二层交换机上。当VLAN间的主机需要通信时，数据会经由路由器进行三层路由，并被转发到目的VLAN内的主机，这样就可以实现VLAN之间的相互通信。

然而，随着每个交换机上VLAN数量的增加，这样做必然需要大量的路由器接口，而路由器的接口数量是极其有限的。并且，某些VLAN之间的主机可能不需要频繁进行通信，如果这样配置的话，会导致路由器的接口利用率很低。因此，实际应用中一般不会采用这种方案来解决VLAN间的通信问题。

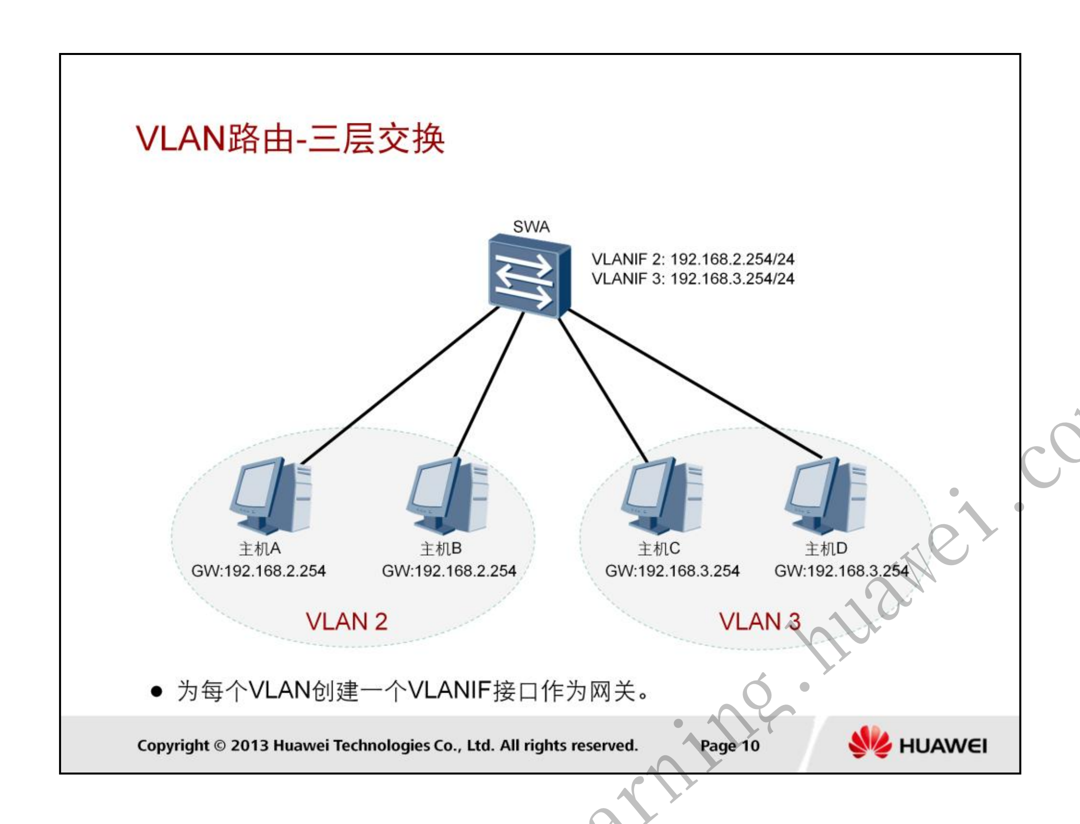


解决VLAN间通信问题的第二种方法是：

在交换机和路由器之间仅使用一条物理链路连接。在交换机上，把连接到路由器的端口配置成Trunk类型的端口，并允许相关VLAN的帧通过。在路由器上需要创建子接口，逻辑上把连接路由器的物理链路分成了多条。一个子接口代表了一条归属于某个VLAN的逻辑链路。配置子接口时，需要注意以下几点：

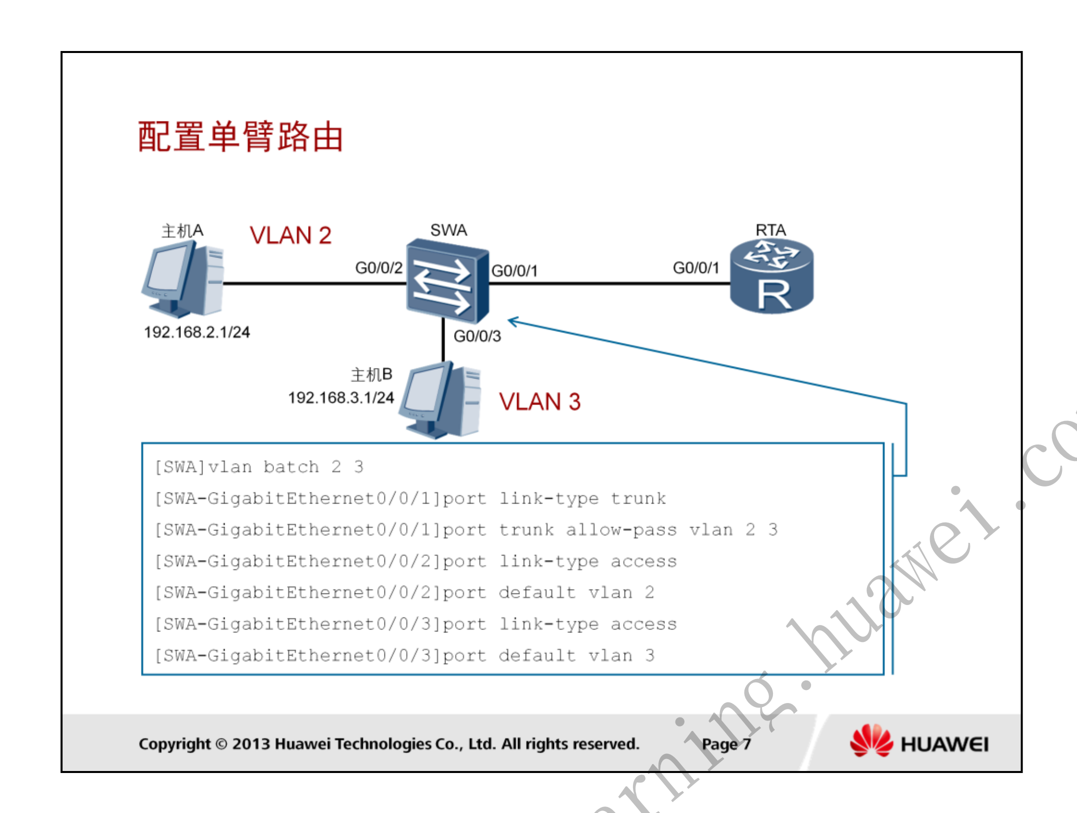
1. 必须为每个子接口分配一个IP地址。该IP地址与子接口所属VLAN位于同一网段。
2. 需要在子接口上配置802.1Q封装，来剥掉和添加VLAN Tag，从而实现VLAN间互通。
3. 在子接口上执行命令**arp broadcast enable**使能子接口的ARP广播功能。

本例中，主机A发送数据给主机B时，RTA会通过G0/0/1.1子接口收到此数据，然后查找路由表，将数据从G0/0/1.2子接口发送给主机B，这样就实现了VLAN2和VLAN3之间的主机通信。



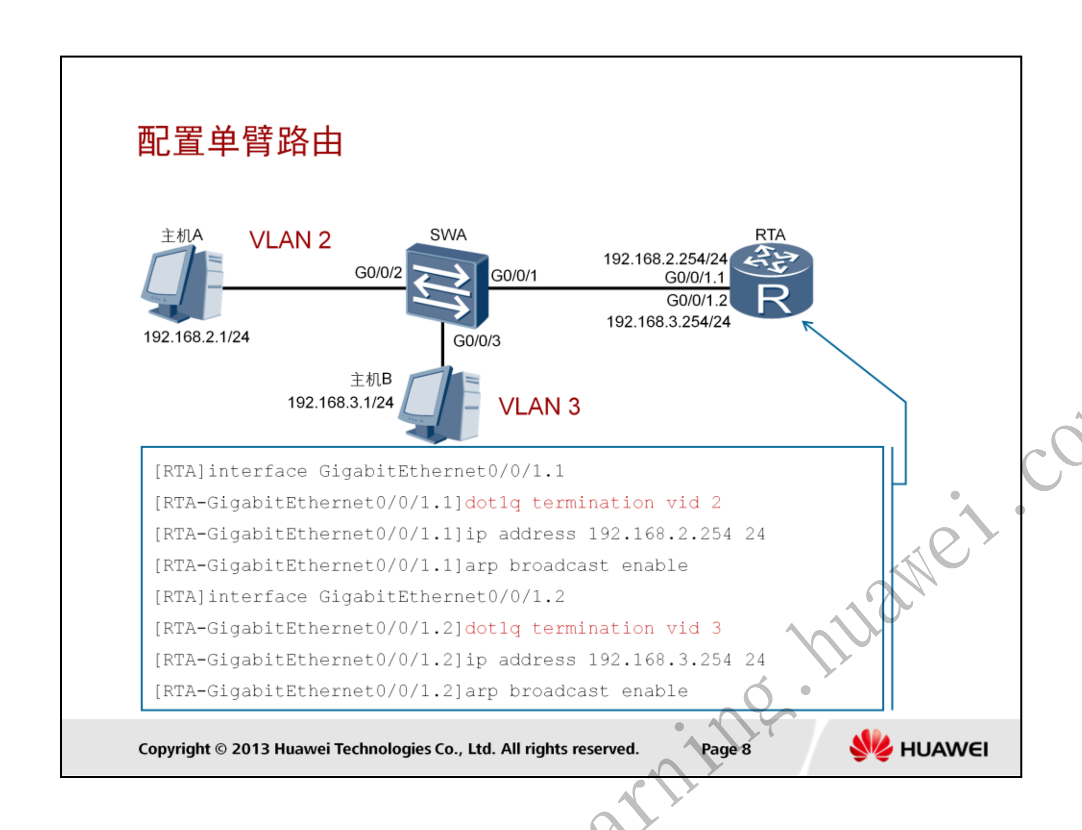
解决VLAN间通信问题的第三种方法是：

在三层交换机上配置VLANIF接口来实现VLAN间路由。如果网络上有多个VLAN，则需要给每个VLAN配置一个VLANIF接口，并给每个VLANIF接口配置一个IP地址。用户设置的缺省网关就是三层交换机中VLANIF接口的IP地址。



执行**port link-type trunk**命令，配置SWA的G0/0/1端口为Trunk类型的端口。

执行**port trunk allow-pass vlan 2 3**命令，配置SWA的G0/0/1端口允许VLAN 2和VLAN 3的数据通过。



interface *interface-type interface-number.sub-interface number*命令用来创建子接口。*sub-interface number*代表物理接口内的逻辑接口通道。

dot1q termination *vid*命令用来配置子接口dot1q封装的单层VLAN ID。缺省情况，子接口没有配置dot1q封装的单层VLAN ID。本命令执行成功后，终结子接口对报文的处理如下：接收报文时，剥掉报文中携带的Tag后进行三层转发。转发出去的报文是否带Tag由出接口决定。发送报文时，将相应的VLAN信息添加到报文中再发送。

arp broadcast enable命令用来使能终结子接口的ARP广播功能。缺省情况下，终结子接口没有使能ARP广播功能。终结子接口不能转发广播报文，在收到广播报文后它们直接把该报文丢弃。为了允许终结子接口能转发广播报文，可以通过在子接口上执行此命令。

配置验证

```
Host A>ping 192.168.3.1

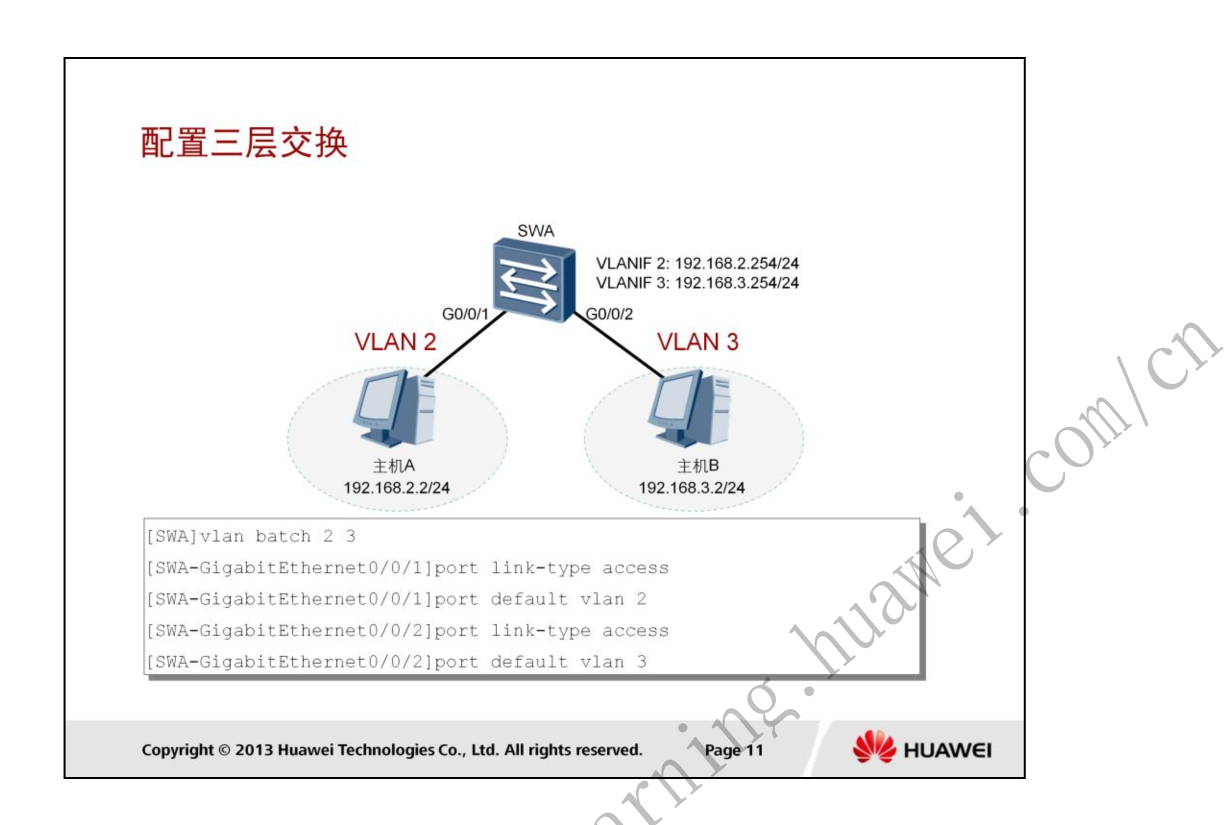
Ping 192.168.3.1: 32 data bytes, Press Ctrl_C to break
From 192.168.3.1: bytes=32 seq=1 ttl=127 time=15 ms
From 192.168.3.1: bytes=32 seq=2 ttl=127 time=15 ms
From 192.168.3.1: bytes=32 seq=3 ttl=127 time=32 ms
From 192.168.3.1: bytes=32 seq=4 ttl=127 time=16 ms
From 192.168.3.1: bytes=32 seq=5 ttl=127 time=31 ms

--- 192.168.3.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/21/32 ms
```

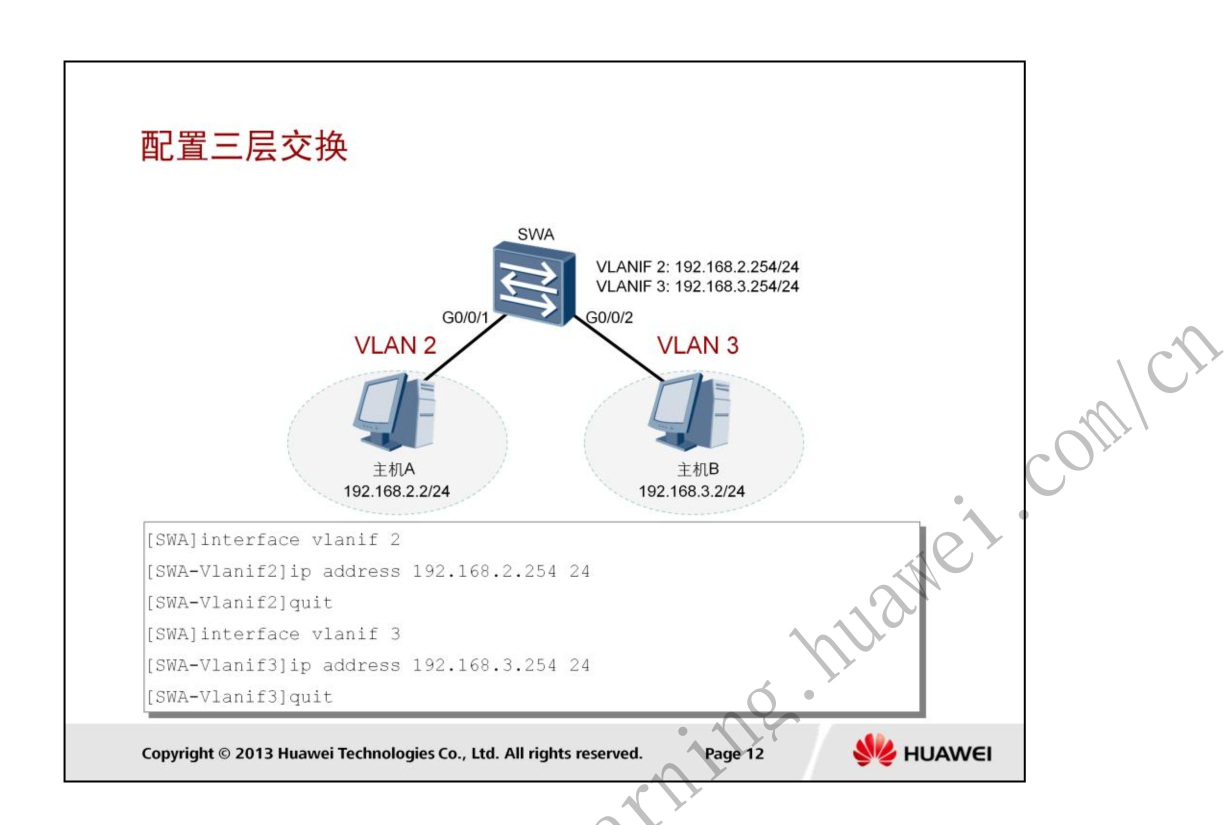

Page 10



配置完成单臂路由后，可以使用**ping**命令来验证主机之间的连通性。如上所示，VLAN2中的主机A(IP地址：192.168.2.1）可以Ping通VLAN 3中的主机B(IP地址：192.168.3.1)。



在三层交换机上配置VLAN路由时，首先创建VLAN，并将端口加入到VLAN中。



interface vlanif *vlan-id*命令用来创建VLANIF接口并进入到VLANIF接口视图。*vlan-id*表示与VLANIF接口相关联的VLAN编号。VLANIF接口的IP地址作为主机的网关IP地址，和主机的IP地址必须位于同一网段。

配置验证

```
Host A>ping 192.168.3.2

Ping 192.168.3.2: 32 data bytes, Press Ctrl_C to break
From 192.168.3.2: bytes=32 seq=1 ttl=127 time=15 ms
From 192.168.3.2: bytes=32 seq=2 ttl=127 time=15 ms
From 192.168.3.2: bytes=32 seq=3 ttl=127 time=32 ms
From 192.168.3.2: bytes=32 seq=4 ttl=127 time=16 ms
From 192.168.3.2: bytes=32 seq=5 ttl=127 time=31 ms

--- 192.168.3.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/21/32 ms
```

 Page 13



配置三层交换后，可以用**ping**命令验证主机之间的连通性。如上所示，VLAN2中的主机A(IP地址：192.168.2.2）可以Ping通VLAN 3中的主机B(IP地址：192.168.3.2)。



总结

- 配置命令dot1q termination vid <vlan-id> 的目的是什么？
- 配置单臂路由时，交换机连接路由器的接口需要哪些配置？



1. **dot1q termination vid** *vlan-id*命令有两个功能。第一个功能是删除VLAN标签。接口在收到VLAN报文后，剥掉报文中携带的Tag后进行三层转发。第二个功能是添加VLAN标签。接口在发送报文时，将相应的VLAN信息添加到报文中再发送。
2. 必须把接口配置成Trunk口，并允许相应VLAN的数据通过。


谢谢
www.huawei.com


WLAN概述
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

无线局域网WLAN（Wireless Local Area Network）是一种利用无线技术实现主机等终端设备灵活接入以太网的技术，它使得网络的构建和终端的移动更加的方便和灵活。 WLAN不仅可以作为有线局域网的补充和延伸，而且还可以与有线网络互为备份。

 Page 2





学习目标

学完本课程后，您应该:

- 理解WLAN在企业网络中的应用

WLAN的应用









- 随着WLAN技术的发展，人们可以使用越来越多的移动设备接入到企业网络中进行办公，大大提高了工作效率。

 Page 4



无线局域网技术发展迅猛，在许多企业网络中都已经普及。未来，无线局域网在企业网络中有望取代有线以太网，为用户提供无处不在的网络接入。平板电脑和智能移动设备的使用热潮为BYOD（Bring Your Own Device）解决方案的推广铺平了道路，并带来了企业领域工作方式的改变。BYOD是指自带设备进行办公，这些设备包括个人电脑、手机、平板等智能终端，通过这些智能终端，员工可以在任何地方，任何地点进行收发公司邮件，访问公司资源，对公司的业务进行处理，实现移动办公。

。BYOD解决方案可以为用户提供一个无处不在的网络，支持不同种类的自带设备安全地访问企业网络，保持自带设备的良好用户体验，提升用户满意度和工作效率。

无线网络在普及的同时也面临着众多挑战。例如，如何实现高密度的设备接入；如何避免信号损耗和连接中断以保障媒体业务（语音和视频）的流畅性；如何防御网络入侵，保证用户的接入安全。



无线网络的初步应用，可以追朔到第二次世界大战期间，当时美国陆军采用了无线电信号来进行资料的传输。他们研发出了一套高强度加密的无线电传输系统，该系统在美军和盟军中得到了广泛的使用。他们也许没有想到，这项技术会在几十年后的今天改变我们的生活。1971年，夏威夷大学的研究人员研发出了第一个基于封包式技术的无线电通讯网络，称为ALOHAnet。它包括了7台计算机，采用双向星型拓扑横跨四座夏威夷的岛屿，中心计算机放置在瓦胡岛上。一般认为，ALOHAnet的出现，标志了无线局域网的正式诞生。

1990年，IEEE正式启动了802.11项目，无线局域网技术逐渐走向成熟。IEEE802.11(WiFi)标准诞生以来，先后有802.11a，802.11b，802.11g，802.11e，802.11f，802.11h，802.11i，802.11j等标准被制定出来，目前802.11n的应用已经非常普遍，802.11n技术可以提供用户高速度、高质量的WLAN服务。

2003年以来，无线网络市场热度迅速飙升，已经成为IT市场中新的增长亮点。由于人们对网络速度及方便使用性的期望越来越大，于是与电脑以及移动设备结合紧密的WiFi、CDMA/GPRS、蓝牙等技术越来越受到人们的追捧。与此同时，在相应配套产品大量面世之后，构建无线网络所需要的成本下降了，一时间，无线网络已经成为我们生活的主流。

目前，随着3G、4G（LTE）等高速移动网络的面市，移动网络成为生活中的不可缺少的一部分，很多商店、餐馆等公共场所也提供了很多WiFi无线热点。

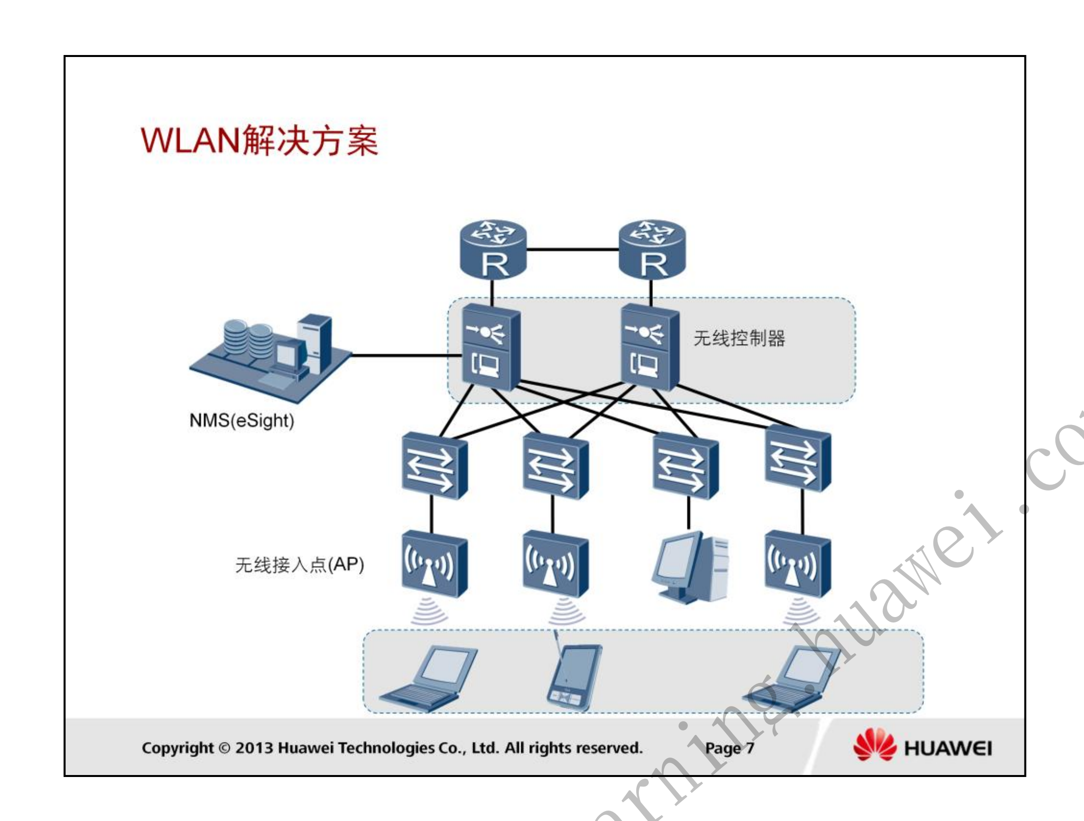
IEEE 802.11主要标准

版本	年份	频段	速率
802.11-1997	1997	2.4 GHz	2 Mbps
802.11 a	1999	5 GHz	54 Mbps
802.11 b	1999	2.4 GHZ	11 Mbps
802.11 g	2003	2.4 GHz	54 Mbps
802.11 n	2009	2.4 GHz 5 GHz	600 Mbps
802.11 ac	2013	5 GHz	> 1 Gbps

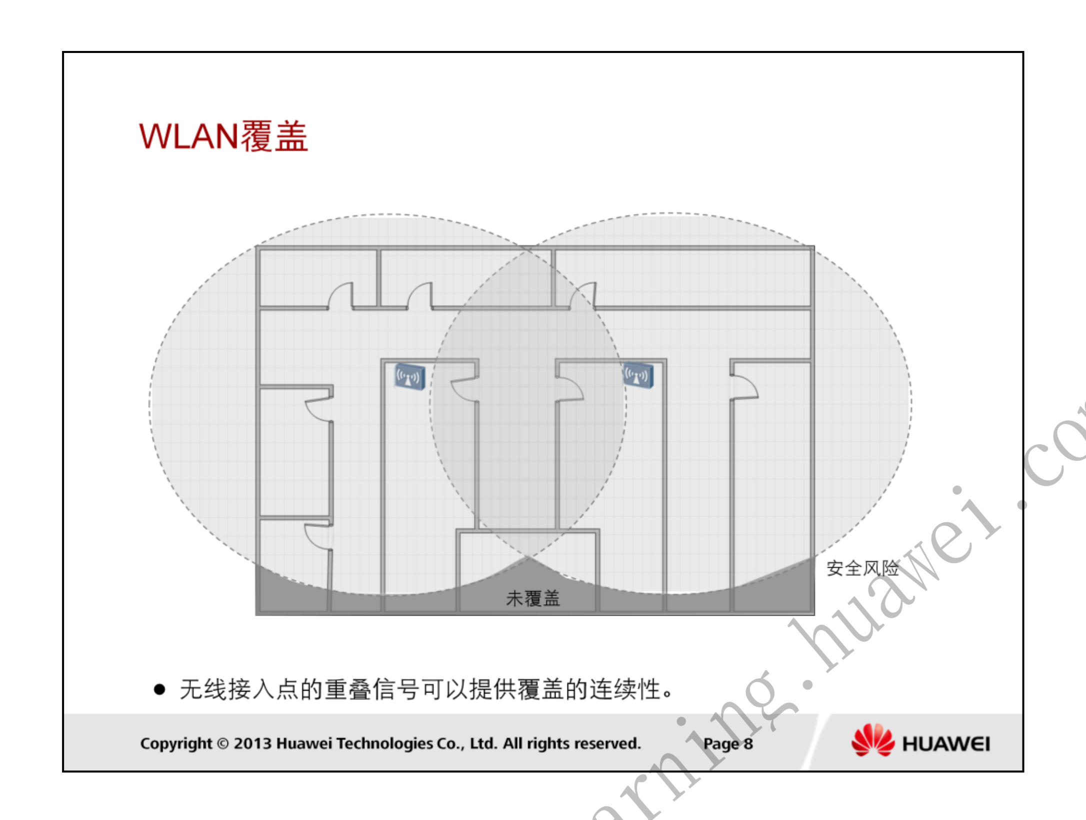
 Page 6



802.11协议组是国际电工电子工程学会（IEEE）专门为无线局域网络制定的标准。原始标准制定于1997年，工作在2.4GHz频段，速率最高只能达到2Mbps。随后IEEE又相继开发了802.11a和802.11b两个标准，分别工作在5GHz和2.4GHz频段。这两个标准提供的信号范围有差异。5GHz频段信号衰减严重，速率高，但是抗干扰能力差，传输距离较短。2.4GHz频段抗衰减能力强，传输距离较远，因而允许在较大的范围内部署更少的AP。之后，IEEE还发布了802.11g，802.11n和802.11ac标准。

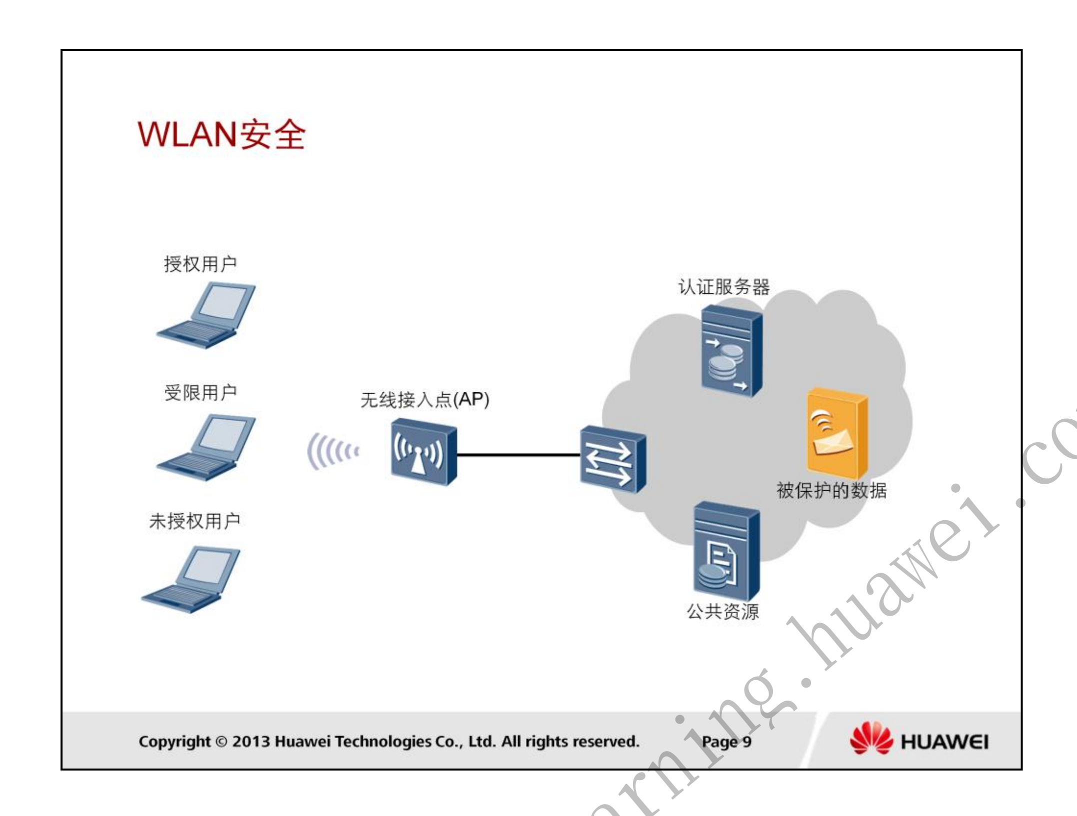


中小企业园区一般面积有限，因而通常只需要部署一个两层架构的小型无线网络就可以满足用户接入网络的需求。接入控制器一般旁挂在网络的核心层，而不是直接连接接入点，这样既可以达到无线网络叠加的目的，同时也能降低对现有企业网络的影响。



每个接入点只能覆盖一定的周边面积。因为受到各种因素以及障碍物的影响，各个接入点的覆盖面积还会有所差异。障碍物会造成信号衰减，引起信号反射进而影响信号覆盖范围。因此，为了扩大覆盖面积，一般将多个AP作为独立的单元同时部署，提供重叠的覆盖区域，允许用户在几个AP的覆盖面积内移动时可以无缝漫游。合理的无线部署能够实现整个园区的全面覆盖，消除覆盖盲区。

无线覆盖同时也需要考虑网络安全问题。不同于有线以太连接，无线网络的范围超出建筑物或局点的物理边界之外时，未知的外部用户在没有经过授权的情况下可能获取到无线资源，从而带来网络安全风险。



为了维护无线企业网络的安全性，IEEE 设计了多种安全机制。

边界安全机制是一种典型的无线安全解决方案，能够保护802.11网络不受来自非法AP、非法用户、DoS攻击的威胁。

无线入侵检测系统可以用来检测非法用户和非法AP，无线入侵防御系统则可以保护企业网络来防御非法接入。

用户接入安全解决方案则运用链路认证，接入认证和数据加密等网络接入控制方式，保证数据的有效性和用户的接入安全，通过定义用户权限来管理用户接入。

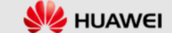
业务安全是无线网络的另一个安全特性，用以在数据传输过程中防止合法用户的数据被非法用户窃取。



总结

- 在企业网络中部署WLAN的优势有哪些?
- 在部署WLAN时，需要考虑哪些问题?

 Page 10



1. 大多数员工希望能够实现移动办公，既方便远程会议又方便协同合作。固定的有线网络限制了办公的灵活性，接入企业网络的用户数量也受制于有线连接。而无线局域网则允许员工移动办公，灵活接入。
2. 灵活接入同时也带来了更大的安全风险，因此无线企业网络需要监控用户接入，以保证用户的接入安全，防止公司的敏感信息被窃取。越来越多的员工开始使用私人设备通过无线局域网接入到企业网络，这使企业网络更容易受到病毒、恶意软件、间谍软件的攻击，成为企业网络最大的安全隐患。为了支持更多的业务和用户，无线局域网需要提供更高的带宽，因而需要更多的无线频谱资源。


谢谢
www.huawei.com

Module-2

丰富企业网络间的互联方式


HDLC&PPP原理与配置
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

广域网中经常会使用串行链路来提供远距离的数据传输，高级数据链路控制HDLC（ High-Level Data Link Control ）和点对点协议PPP（ Point to Point Protocol）是两种典型的串口封装协议。

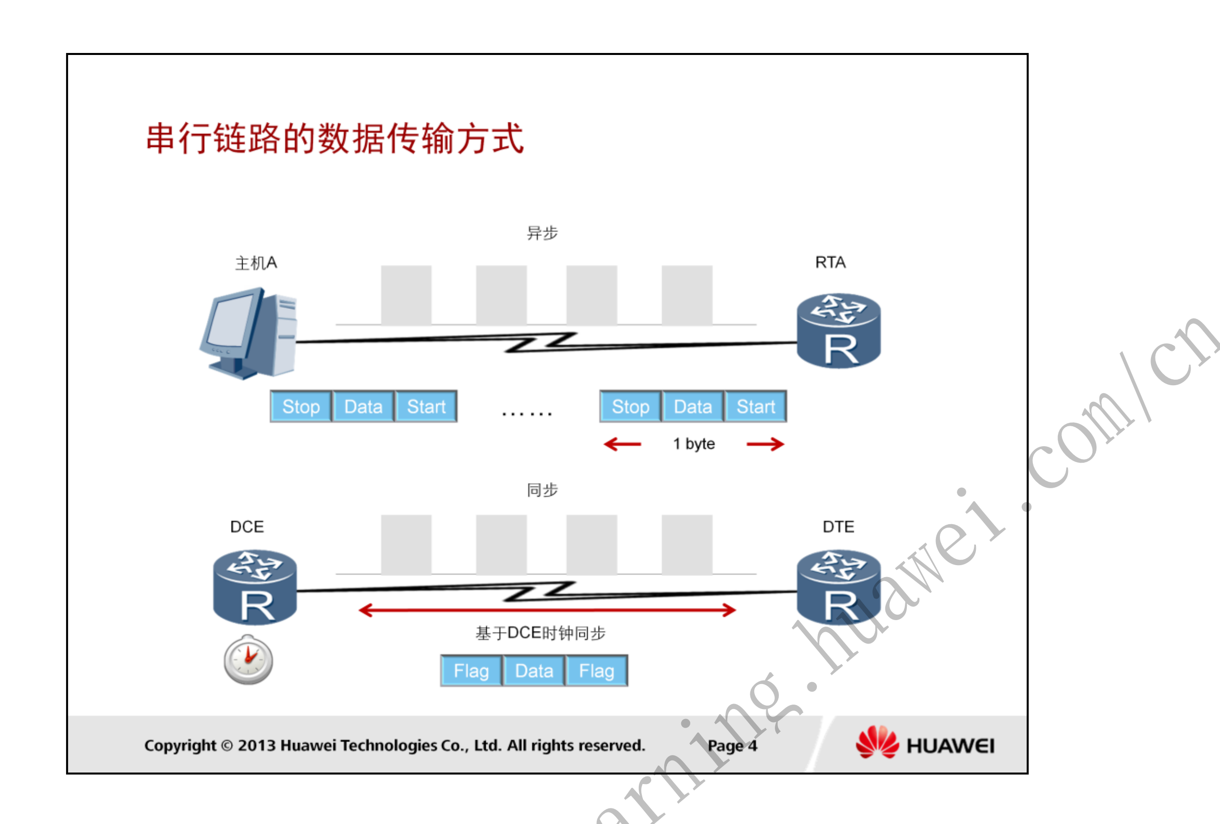




学习目标

学完本课程后，您应该能：

- 掌握HDLC和PPP的工作原理
- 掌握HDLC和PPP的基本配置

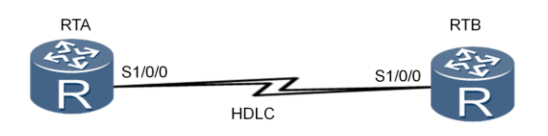


串行链路普遍用于广域网中。串行链路中定义了两种数据传输方式：异步和同步。

异步传输是以字节为单位来传输数据，并且需要采用额外的起始位和停止位来标记每个字节的开始和结束。起始位为二进制值0，停止位为二进制值1。在这种传输方式下，开始和停止位占据发送数据的相当大的比例，每个字节的发送都需要额外的开销。

同步传输是以帧为单位来传输数据，在通信时需要使用时钟来同步本端和对端的设备通信。DCE即数据通信设备，它提供了一个用于同步DCE设备和DTE设备之间数据传输的时钟信号。DTE即数据终端设备，它通常使用DCE产生的时钟信号。

HDLC协议应用

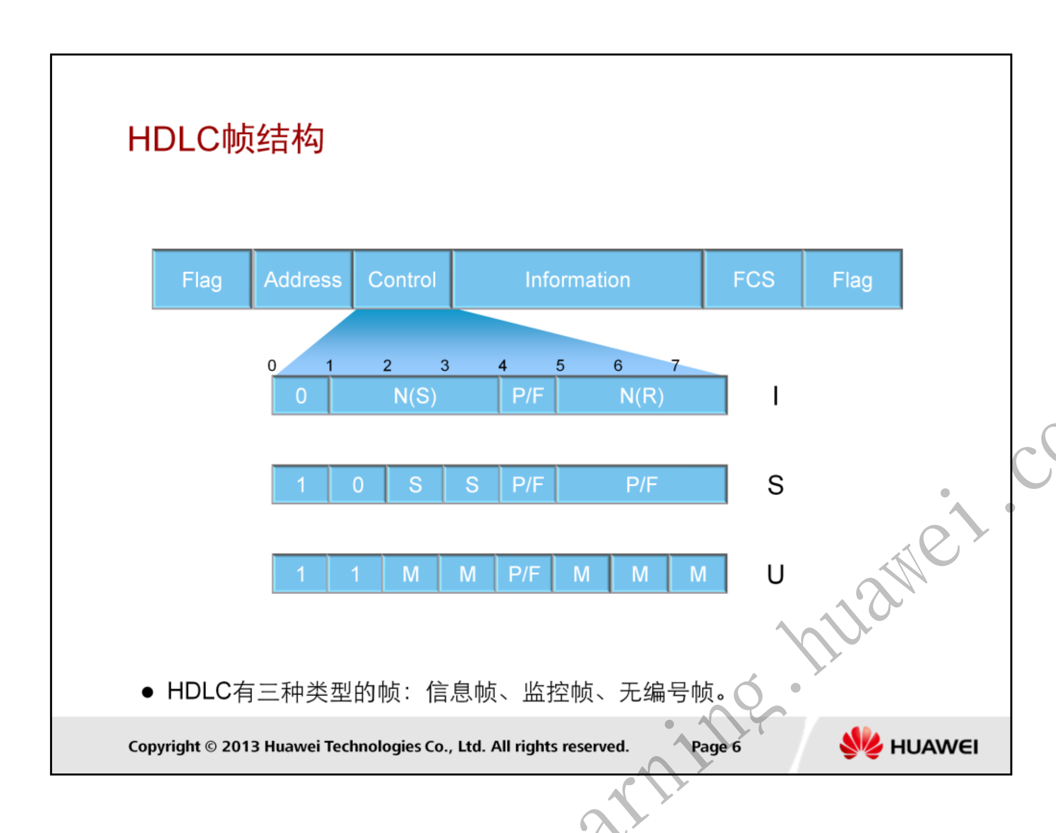


- High-level Data Link Control，高级数据链路控制，简称HDLC，是一种面向比特的链路层协议。


Page 5


ISO制定的HDLC是一种面向比特的通信规则。HDLC传送的信息单位为帧。作为面向比特的同步数据控制协议的典型，HDLC具有如下特点：

1. 协议不依赖于任何一种字符编码集；
2. 数据报文可透明传输，用于透明传输的“0比特插入法”易于硬件实现；
3. 全双工通信，不必等待确认可连续发送数据，有较高的数据链路传输效率；
4. 所有帧均采用CRC校验，并对信息帧进行编号，可防止漏收或重收，传输可靠性高；
5. 传输控制功能与处理功能分离，具有较大的灵活性和较完善的控制功能。

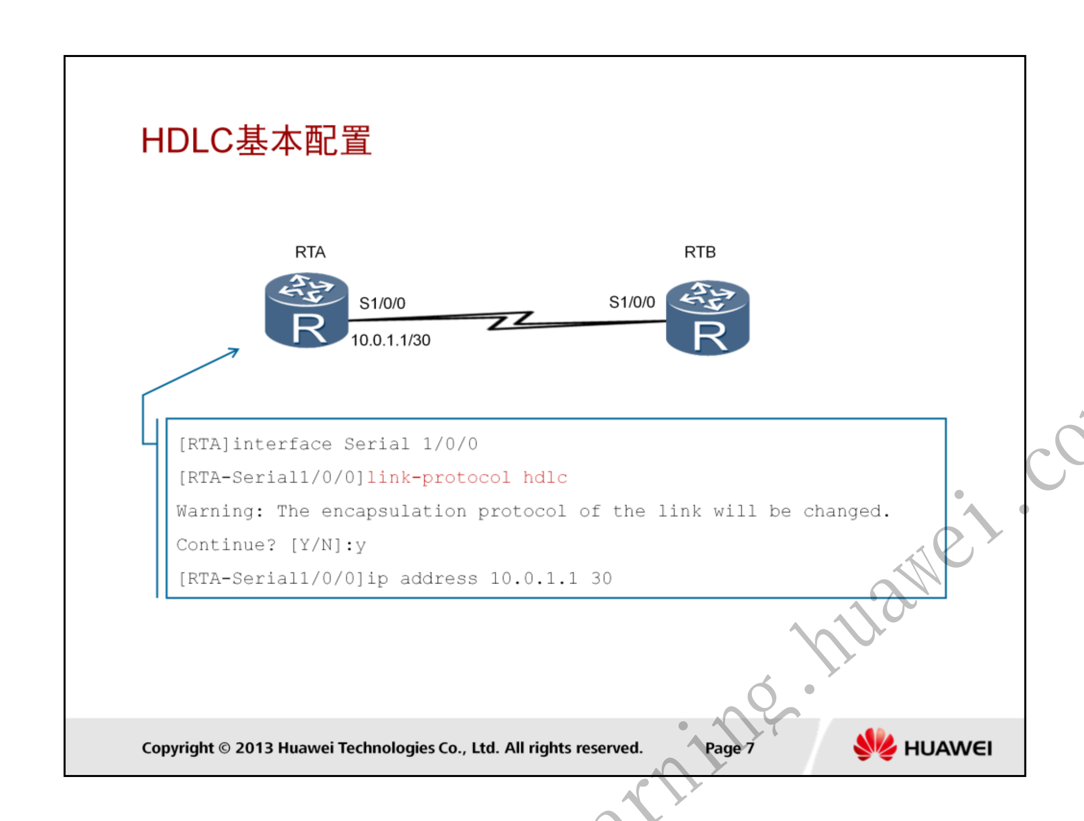


完整的HDLC帧由标志字段（F）、地址字段（A）、控制字段（C）、信息字段（I）、帧校验序列字段（FCS）等组成。

1. 标志字段为01111110，用以标志帧的开始与结束，也可以作为帧与帧之间的填充字符。
2. 地址字段携带的是地址信息。
3. 控制字段用于构成各种命令及响应，以便对链路进行监视与控制。发送方利用控制字段来通知接收方来执行约定的操作；相反，接收方用该字段作为对命令的响应，报告已经完成的操作或状态的变化。
4. 信息字段可以包含任意长度的二进制数，其上限由FCS字段或通讯节点的缓存容量来决定，目前用得较多的是1000-2000比特，而下限可以是0，即无信息字段。监控帧中不能有信息字段。
5. 帧检验序列字段可以使用16位CRC对两个标志字段之间的内容进行校验。

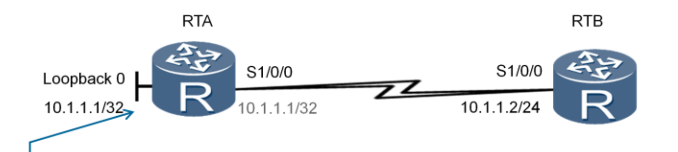
HDLC有三种类型的帧：

1. 信息帧（I帧）用于传送有效信息或数据，通常简称为I帧。
2. 监控帧（S帧）用于差错控制和流量控制，通常称为S帧。S帧 的 标志是控制字段的前两个比特位为“10”。S帧不带信息字段，只有6个字节即48个比特。
3. 无编号帧（U帧）简称U帧。U帧用于提供对链路的建立、拆除以及多种控制功能。



用户只需要在串行接口视图下运行**link-protocol** hdlc命令就可以使能接口的HDLC协议。华为设备上的串行接口默认运行PPP协议。用户必须在串行链路两端的端口上配置相同的链路协议，双方才能通信。

HDLC接口地址借用




```
[RTA]interface Serial 1/0/0
[RTA-Serial1/0/0]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y
[RTA-Serial1/0/0]ip address unnumbered interface loopBack 0
[RTA]ip route-static 10.1.1.0 24 Serial 1/0/0
```

- 串行接口可以借用Loopback接口的IP地址和对端建立连接。



一个接口如果没有IP地址就无法生成路由，也就无法转发报文。IP地址借用允许一个没有IP地址的接口从其它接口借用IP地址。这样可以避免一个接口独占IP地址，节省IP地址资源。一般建议借用loopback接口的IP地址，因为这类接口总是处于活跃（active）状态，因而能提供稳定可用的IP地址。

本例中，在RTA的S1/0/0接口配置完接口地址借用之后，还需要在RTA上配置静态路由，以使RTA能够转发数据到10.1.1.0/24网络。

配置验证

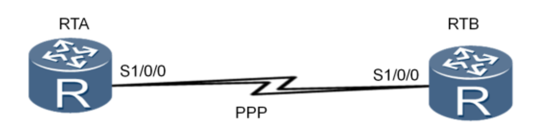
```
[RTA]display ip interface brief
*down: administratively down ^down: standby (l): loopback
(s): spoofing
……
Interface                    IP Address/Mask      Physical    Protocol
LoopBack0                    10.1.1.1/32            up          up(s)
Serial1/0/0                  10.1.1.1/32            up          up
Serial1/0/1                  unassigned             up          down
```

 Page 9



执行**display ip interface brief**命令可以查看路由器接口简要信息。如果有IP地址被借用，该IP地址会显示在多个接口上，说明借用loopback接口的IP地址成功。

PPP协议应用



- PPP协议是一种点到点链路层协议，主要用于在全双工的同异步链路上进行点到点的数据传输。

 Page 10



PPP协议是一种点到点链路层协议，主要用于在全双工的同异步链路上进行点到点的数据传输。PPP协议有如下优点：

1. PPP既支持同步传输又支持异步传输，而X.25、FR（Frame Relay）等数据链路层协议仅支持同步传输，SLIP仅支持异步传输。
2. PPP协议具有很好的扩展性，例如，当需要在以太网链路上承载PPP协议时，PPP可以扩展为PPPoE。
3. PPP提供了LCP（Link Control Protocol）协议，用于各种链路层参数的协商。
4. PPP提供了各种NCP（Network Control Protocol）协议（如IPCP、IPXCP），用于各网络层参数的协商，更好地支持了网络层协议。
5. PPP提供了认证协议：CHAP（Challenge-Handshake Authentication Protocol）、PAP（Password Authentication Protocol），更好的保证了网络的安全性。
6. 无重传机制，网络开销小，速度快。

PPP组件

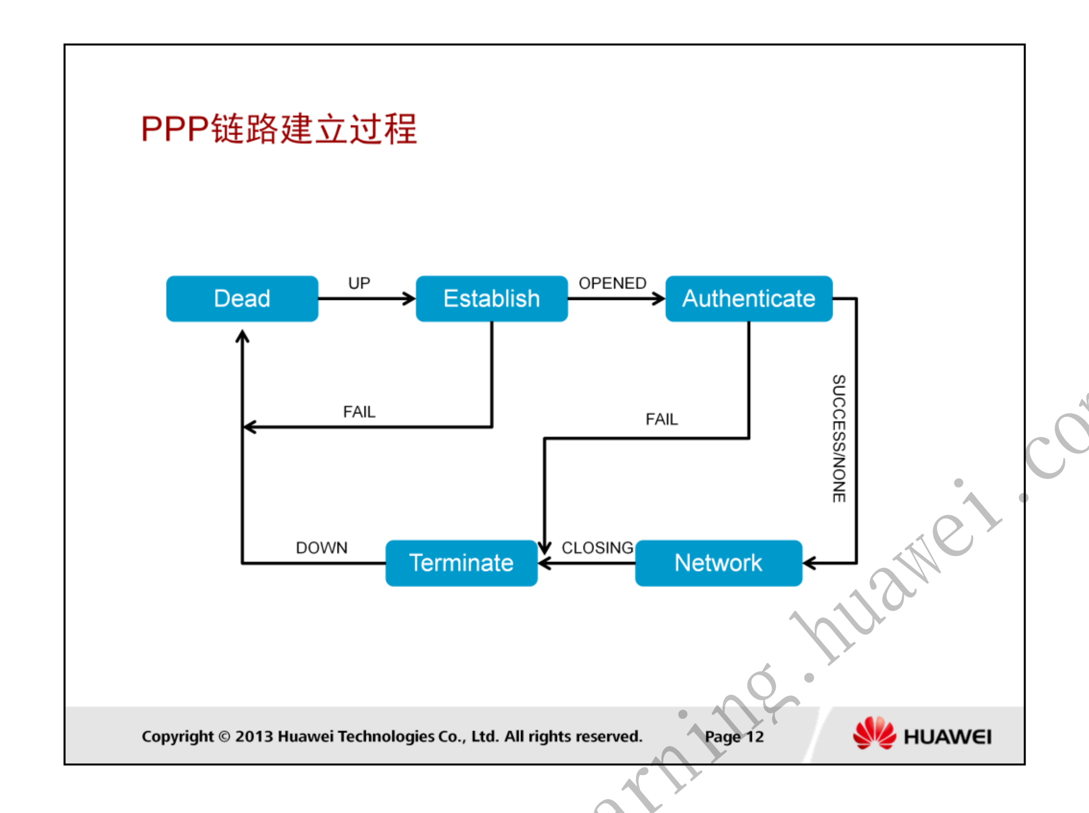
名称	作用
链路控制协议 Link Control Protocol	用来建立、拆除和监控PPP数据链路
网络层控制协议 Network Control Protocol	用于对不同的网络层协议进行连接建立和参数协商



PPP包含两个组件：链路控制协议LCP和网络层控制协议NCP。

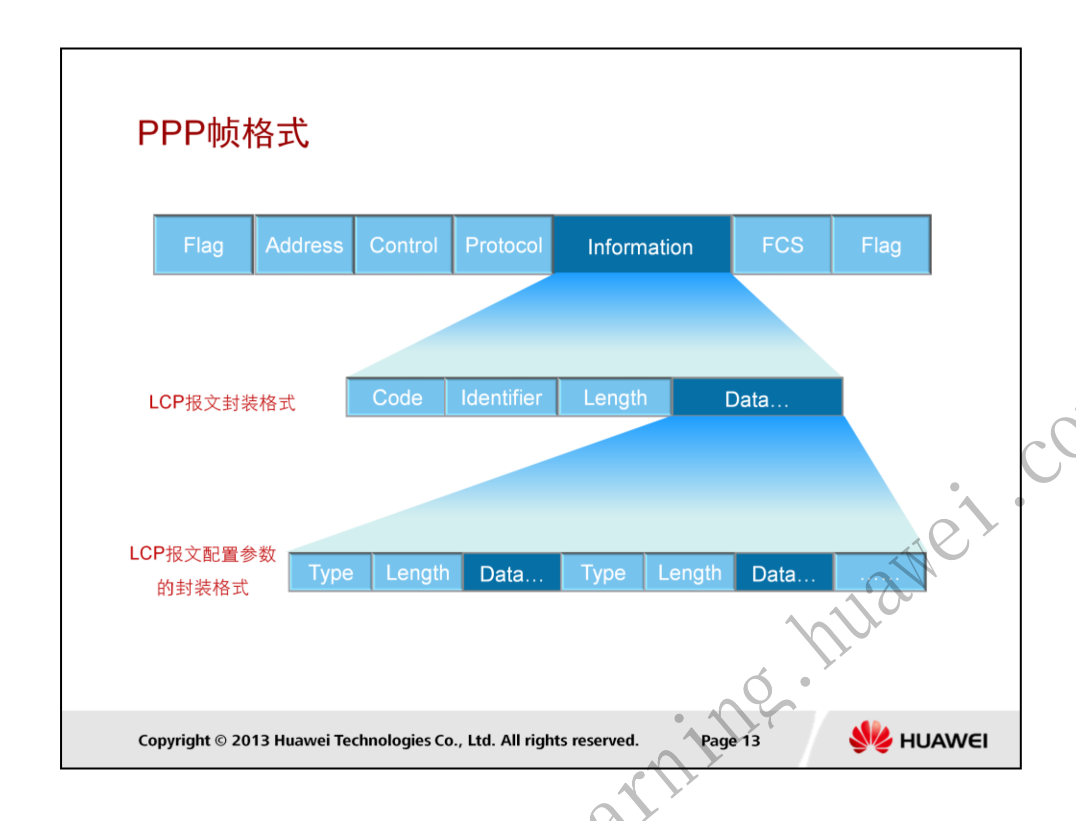
为了能适应多种多样的链路类型，PPP定义了链路控制协议LCP。LCP可以自动检测链路环境，如是否存在环路；协商链路参数，如最大数据包长度，使用何种认证协议等等。与其他数据链路层协议相比，PPP协议的一个重要特点是可以提供认证功能，链路两端可以协商使用何种认证协议来实施认证过程，只有认证成功之后才会建立连接。

PPP定义了一组网络层控制协议NCP，每一个NCP对应了一种网络层协议，用于协商网络层地址等参数，例如IPCP用于协商控制IP协议，IPXCP用于协商控制IPX协议等。



对于PPP链路建立过程的描述如下：

1. Dead阶段也称为物理层不可用阶段。当通信双方的两端检测到物理线路激活时，就会从Dead阶段迁移至Establish阶段，即链路建立阶段。
2. 在Establish阶段，PPP链路进行LCP参数协商。协商内容包括最大接收单元MRU、认证方式、魔术字（Magic Number）等选项。LCP参数协商成功后会进入Opened状态，表示底层链路已经建立。
3. 多数情况下,链路两端的设备是需要经过认证阶段（Authenticate）后才能够进入到网络层协议阶段。PPP链路在缺省情况下是不要求进行认证的。如果要求认证，则在链路建立阶段必须指定认证协议。认证方式是在链路建立阶段双方进行协商的。如果在这个阶段再次收到了Configure-Request报文，则又会返回到链路建立阶段。
4. 在Network阶段，PPP链路进行NCP协商。通过NCP协商来选择和配置一个网络层协议并进行网络层参数协商。只有相应的网络层协议协商成功后，该网络层协议才可以通过这条PPP链路发送报文。如果在这个阶段收到了Configure-Request报文，也会返回到链路建立阶段。
5. NCP协商成功后，PPP链路将保持通信状态。PPP运行过程中，可以随时中断连接，例如物理链路断开、认证失败、超时定时器时间、管理员通过配置关闭连接等动作都可能导致链路进入Terminate阶段。
6. 在Terminate阶段，如果所有的资源都被释放，通信双方将回到Dead阶段，直到通信双方重新建立PPP连接。



PPP采用了与HDLC协议类似的帧格式:

1. Flag域标识一个物理帧的起始和结束，该字节为二进制序列01111110（0X7E）。
2. PPP帧的地址域跟HDLC帧的地址域有差异，PPP帧的地址域字节固定为11111111 （0XFF），是一个广播地址。
3. PPP数据帧的控制域默认为00000011(0X03)，表明为无序号帧。
4. 帧校验序列（FCS）是个16位的校验和，用于检查PPP帧的完整性。
5. 协议字段用来说明PPP所封装的协议报文类型，典型的字段值有：0XC021代表LCP报文，0XC023代表PAP报文，0XC223代表CHAP报文。
6. 信息字段包含协议字段中指定协议的数据包。数据字段的默认最大长度（不包括协议字段）称为最大接收单元MRU（Maximum Receive Unit），MRU的缺省值为1500字节。

如果协议字段被设为0XC021，则说明通信双方正通过LCP报文进行PPP链路的协商和建立:

1. Code字段，主要是用来标识LCP数据报文的类型。典型的报文类型有：配置信息报文（Configure Packets: 0x01），配置成功信息报文(Configure-Ack: 0X02)，终止请求报文(Terminate-Request：0X05)。
2. Identifier域为1个字节，用来匹配请求和响应。

3. Length域的值就是该LCP报文的总字节数据。
4. 数据字段则承载各种TLV（Type/Length/Value）参数用于协商配置选项，包括最大接收单元，认证协议等等。

LCP报文

报文类型	作用
Configure-Request	包含发送者试图与对端建立连接时使用的参数列表
Configure-Ack	表示完全接受对端发送的Configure-Request的参数取值
Configure-Nak	表示对端发送的Configure-Request中的某些参数取值在本端不被认可
Configure-Reject	表示对端发送的Configure-Request中的某些参数本端不能识别

 Page 15



此表格列出了LCP用于链路层参数协商所使用四种报文类型。

1. Configure-Request（配置请求）：链路层协商过程中发送的第一个报文，该报文表明点对点双方开始进行链路层参数的协商。
2. Configure-Ack（配置响应）：收到对端发来的Configure-Request报文，如果参数取值完全接受，则以此报文响应。
3. Configure-Nak（配置不响应）：收到对端发来的Configure-Request报文，如果参数取值不被本端认可，则发送此报文并且携带本端可接受的配置参数。
4. Configure-Reject（配置拒绝）：收到对端发来的Configure-Request报文，如果本端不能识别对端发送的Configure-Request中的某些参数，则发送此报文并且携带那些本端不能认别的配置参数。

LCP协商参数

参数	作用	缺省值
最大接收单元MRU	PPP数据帧中Information字段和Padding字段的总长度	1500字节
认证协议	认证对端使用的认证协议	不认证
魔术字	魔术字为一个随机产生的数字，用于检测链路环路，如果收到的LCP报文中的魔术字和本端产生的魔术字相同，则认为链路有环路	启用

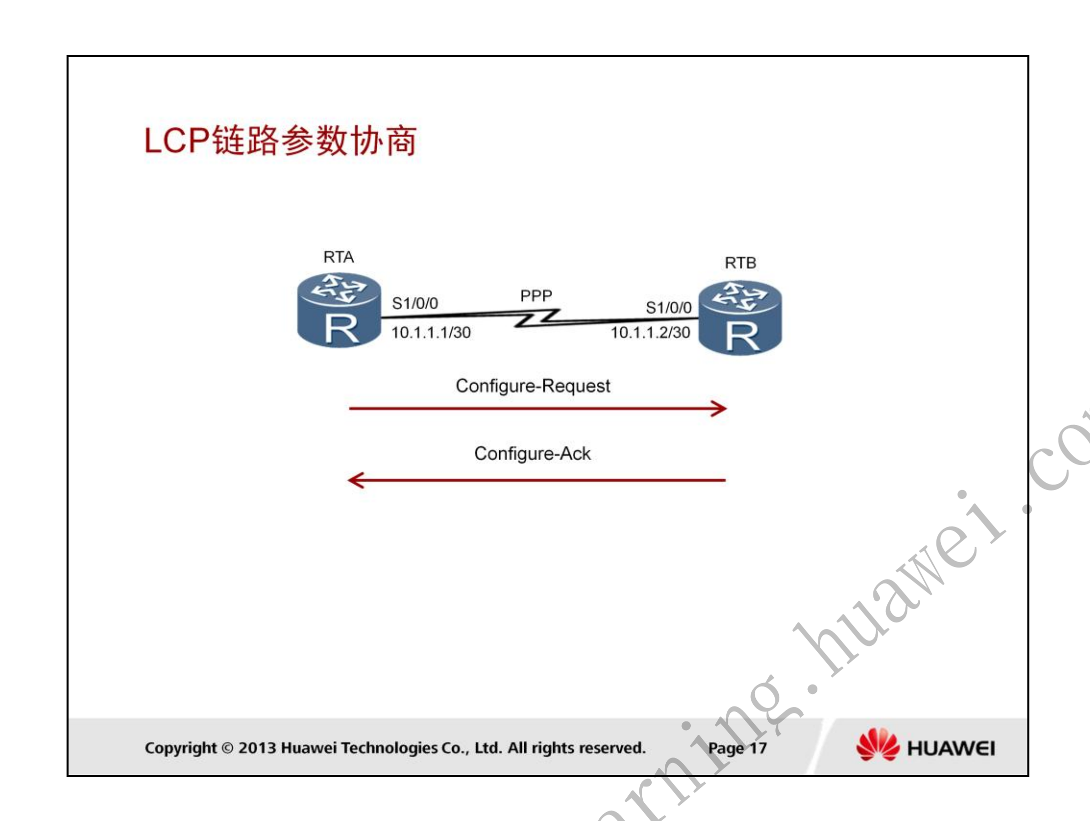
 Page 16



LCP报文携带的一些常见的配置参数有MRU，认证协议，以及魔术字。

1. 在VRP平台上，MRU参数使用接口上配置的最大传输单元（MTU）值来表示。
2. 常用的PPP认证协议有PAP和CHAP，一条PPP链路的两端可以使用不同的认证协议认证对端，但是被认证方必须支持认证方要求使用的认证协议并正确配置用户名和密码等认证信息。
3. LCP使用魔术字来检测链路环路和其它异常情况。魔术字为随机产生的一个数字，随机机制需要保证两端产生相同魔术字的可能性几乎为0。

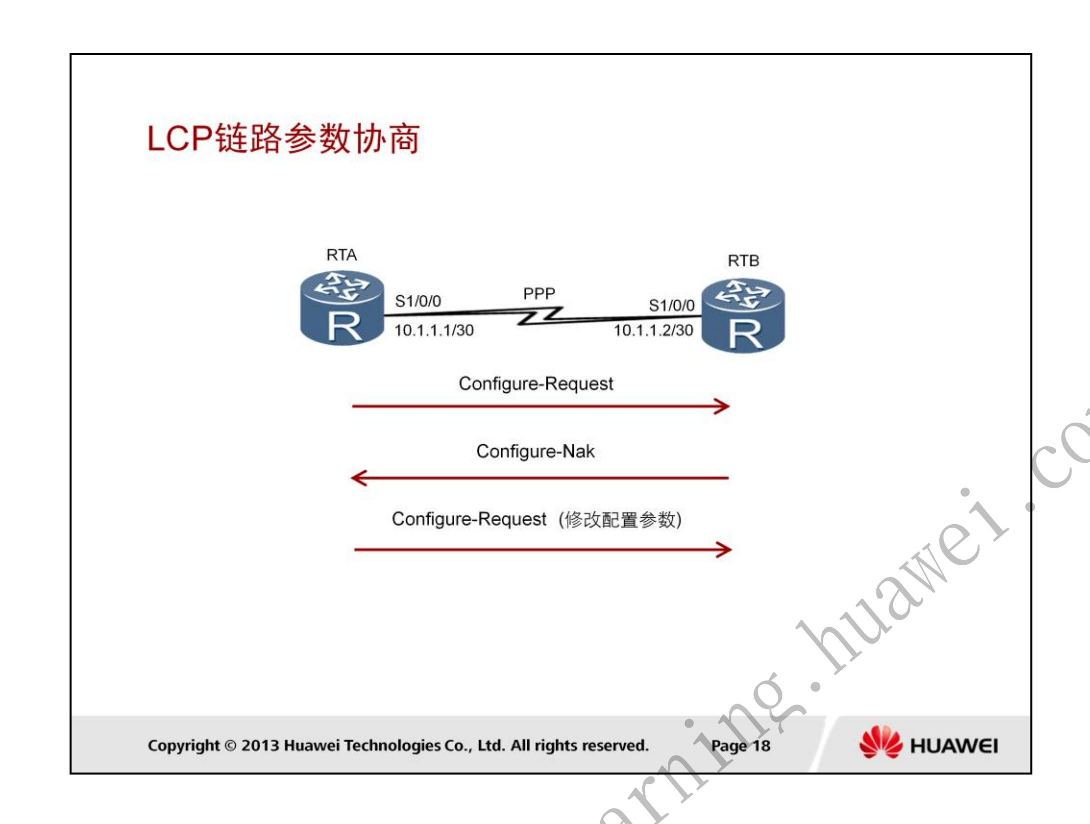
收到一个Configure-Request报文之后，其包含的魔术字需要和本地产生的魔术字做比较，如果不同，表示链路无环路，则使用Confugure-Ack报文确认（其它参数也协商成功），表示魔术字协商成功。在后续发送的报文中，如果报文含有魔术字字段，则该字段设置为协商成功的魔术字。



如图所示，RTA和RTB使用串行链路相连，运行PPP。当物理层链路变为可用状态之后，RTA和RTB使用LCP协商链路参数。本例中，RTA首先发送一个Configure-Request报文，此报文中包含RTA上配置的链路层参数。当RTB收到此Configure-Request报文之后，如果RTB能识别并接受此报文中的所有链路层参数，则向RTA回应一个Configure-Ack报文。

RTA在没有收到Configure-Ack报文的情况下，会每隔3秒重传一次Configure-Request报文，如果连续10次发送Configure-Request报文仍然没有收到Configure-Ack报文，则认为对端不可用，停止发送Configure-Request报文。

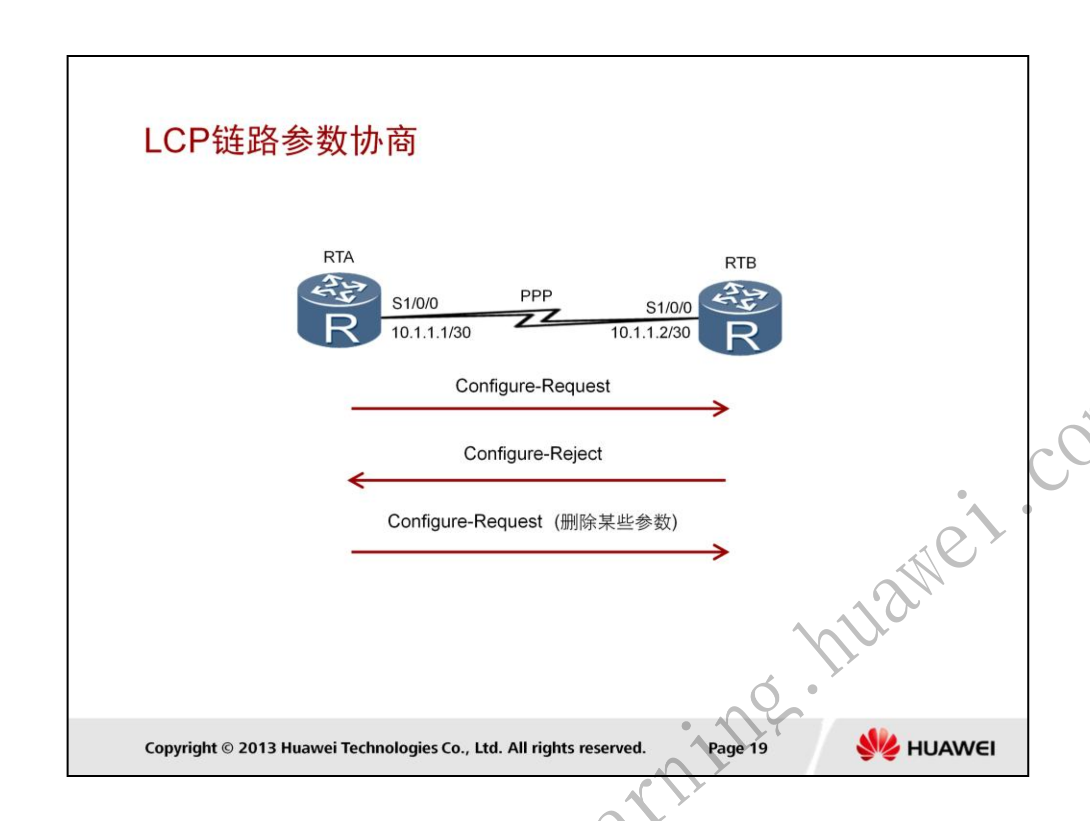
注：完成上述过程只是表明RTB认为RTA上的链路参数配置是可接受的。RTB也需要向RTA发送Configure-Request报文，使RTA检测RTB上的链路参数是不是可接受的。



当RTB收到RTA发送的Configure-Request报文之后，如果RTB能识别此报文中携带的所有链路层参数，但是认为部分或全部参数的取值不能接受，即参数的取值协商不成功，则RTB需要向RTA回应一个Configure-Nak报文。

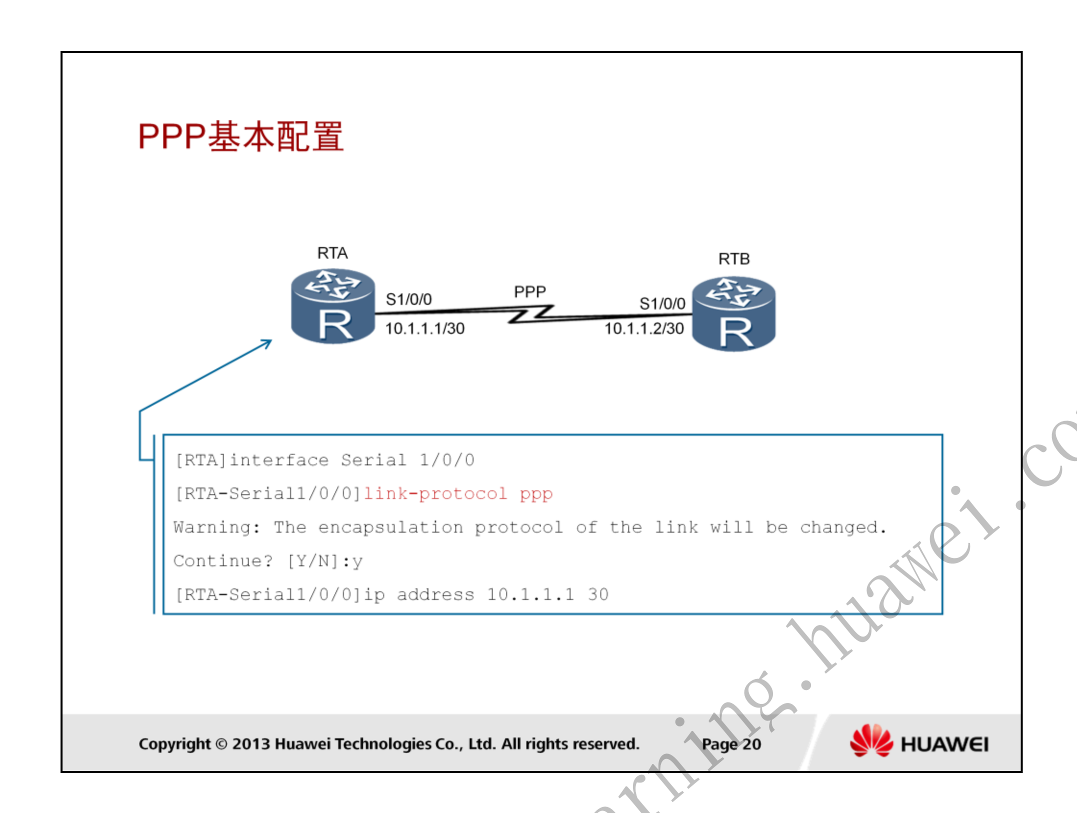
在这个Configure-Nak报文中，只包含不能接受的链路层参数，并且此报文所包含的链路层参数均被修改为RTB上可以接受的取值（或取值范围）。

在收到Configure-Nak报文之后，RTA需要根据此报文中的链路层参数重新选择本地配置的其它参数，并重新发送一个Configure-Request。

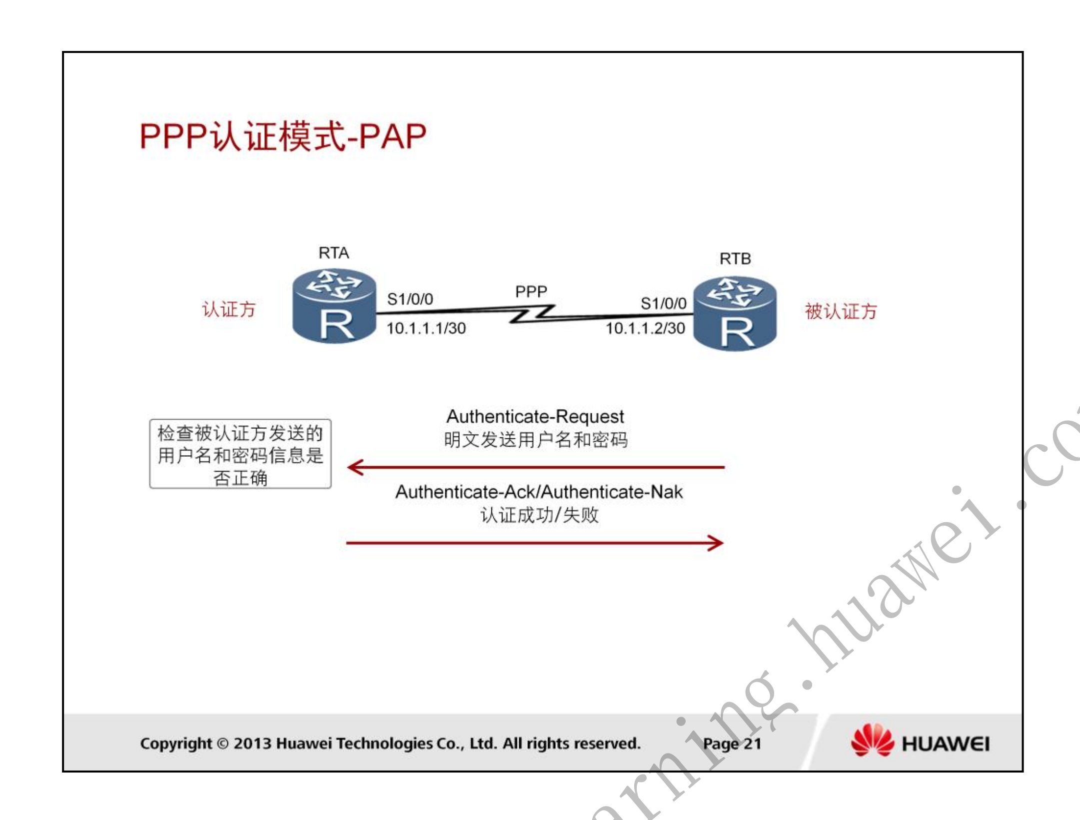


当RTB收到RTA发送的Configure-Request报文之后，如果RTB不能识别此报文中携带的部分或全部链路层参数，则RTB需要向RTA回应一个Configure-Reject报文。在此Configure-Reject报文中，只包含不能被识别的链路层参数。

在收到Configure-Reject报文之后，RTA需要向RTB重新发送一个Configure-Request报文，在新的Configure-Request报文中，不再包含不被对端（RTB）识别的参数。



建立PPP链路之前，必须先在串行接口上配置链路层协议。华为ARG3系列路由器默认在串行接口上使能PPP协议。如果接口运行的不是PPP协议，需要运行**link-protocol ppp**命令来使能数据链路层的PPP协议。

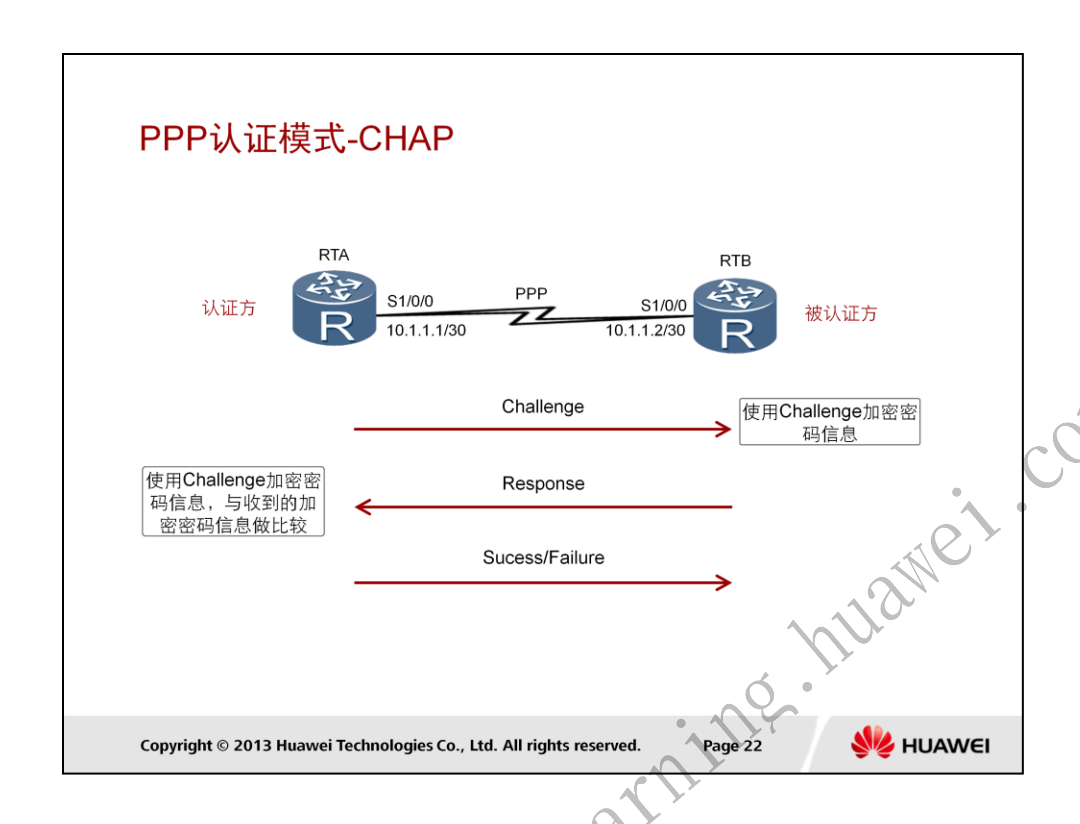


PAP认证的工作原理较为简单。PAP认证协议为两次握手认证协议，密码以明文方式在链路上发送。

LCP协商完成后，认证方要求被认证方使用PAP进行认证。

被认证方将配置的用户名和密码信息使用Authenticate-Request报文以明文方式发送给认证方。

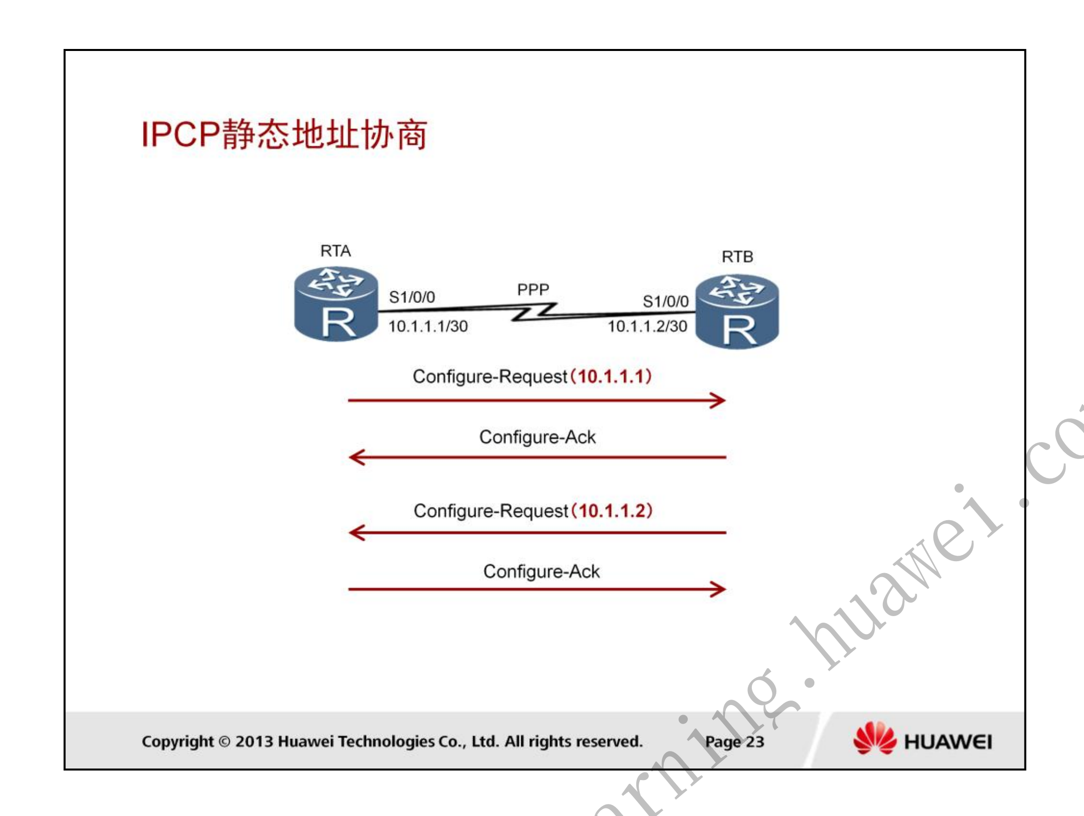
认证方收到被认证方发送的用户名和密码信息之后，根据本地配置的用户名和密码数据库检查用户名和密码信息是否匹配，如果匹配，则返回Authenticate-Ack报文，表示认证成功。否则，返回Authenticate-Nak报文，表示认证失败。



CHAP认证过程需要三次报文的交互。为了匹配请求报文和回应报文，报文中含有Identifier字段，一次认证过程所使用的报文均使用相同的Identifier信息。

1. LCP协商完成后，认证方发送一个Challenge报文给被认证方，报文中含有Identifier信息和一个随机产生的Challenge字符串，此Identifier即为后续报文所使用的Identifier。
2. 被认证方收到此Challenge报文之后，进行一次加密运算，运算公式为MD5{ Identifier＋密码＋Challenge }，意思是将Identifier、密码和Challenge三部分连成一个字符串，然后对此字符串做MD5运算，得到一个16字节长的摘要信息，然后将此摘要信息和端口上配置的CHAP用户名一起封装在Response报文中发回认证方。
3. 认证方接收到被认证方发送的Response报文之后，按照其中的用户名在本地查找相应的密码信息，得到密码信息之后，进行一次加密运算，运算方式和被认证方的加密运算方式相同，然后将加密运算得到的摘要信息和Response报文中封装的摘要信息做比较，相同则认证成功，不相同则认证失败。

使用CHAP认证方式时，被认证方的密码是被加密后才进行传输的，这样就极大的提高了安全性。



IPCP使用和LCP相同的协商机制、报文类型，但IPCP并非调用LCP，只是工作过程、报文等和LCP相同。

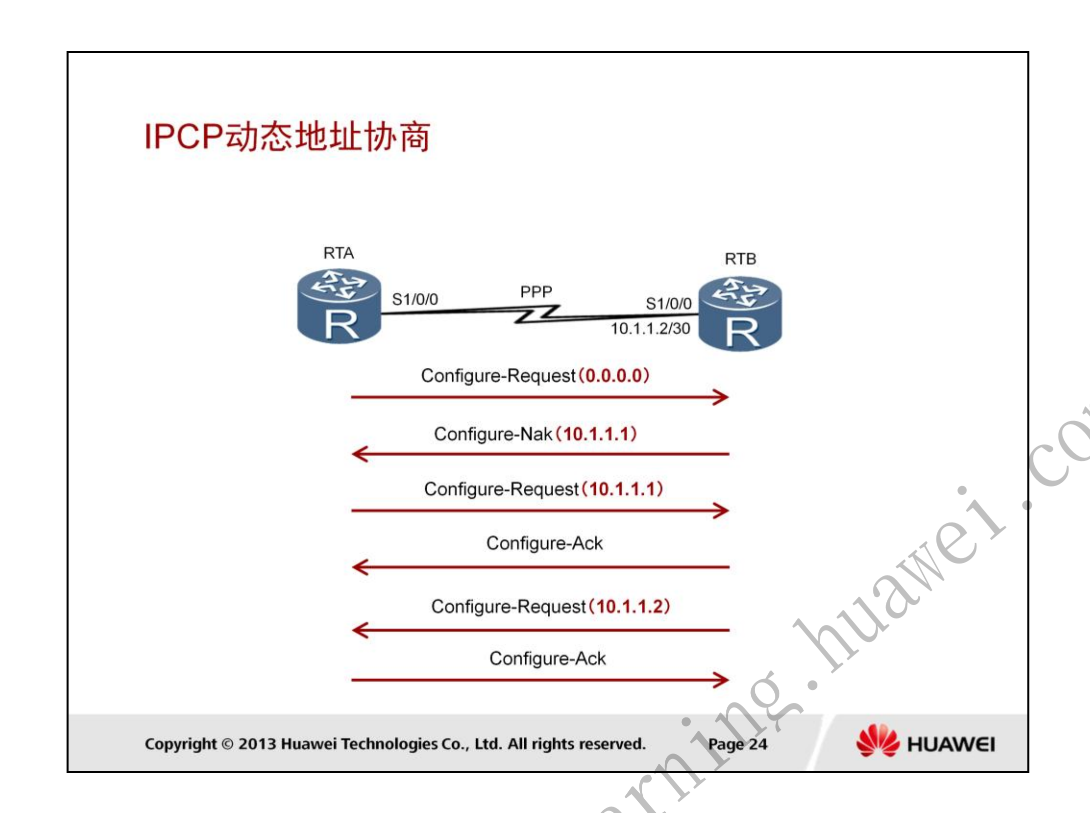
IP地址协商包括两种方式：静态配置协商和动态配置协商。

如图所示，两端路由器配置的IP地址分别为10.1.1.1/30和10.1.1.2/30。

静态IP地址的协商过程如下：

1. 每一端都要发送Configure-Request报文，在此报文中包含本地配置的IP地址；

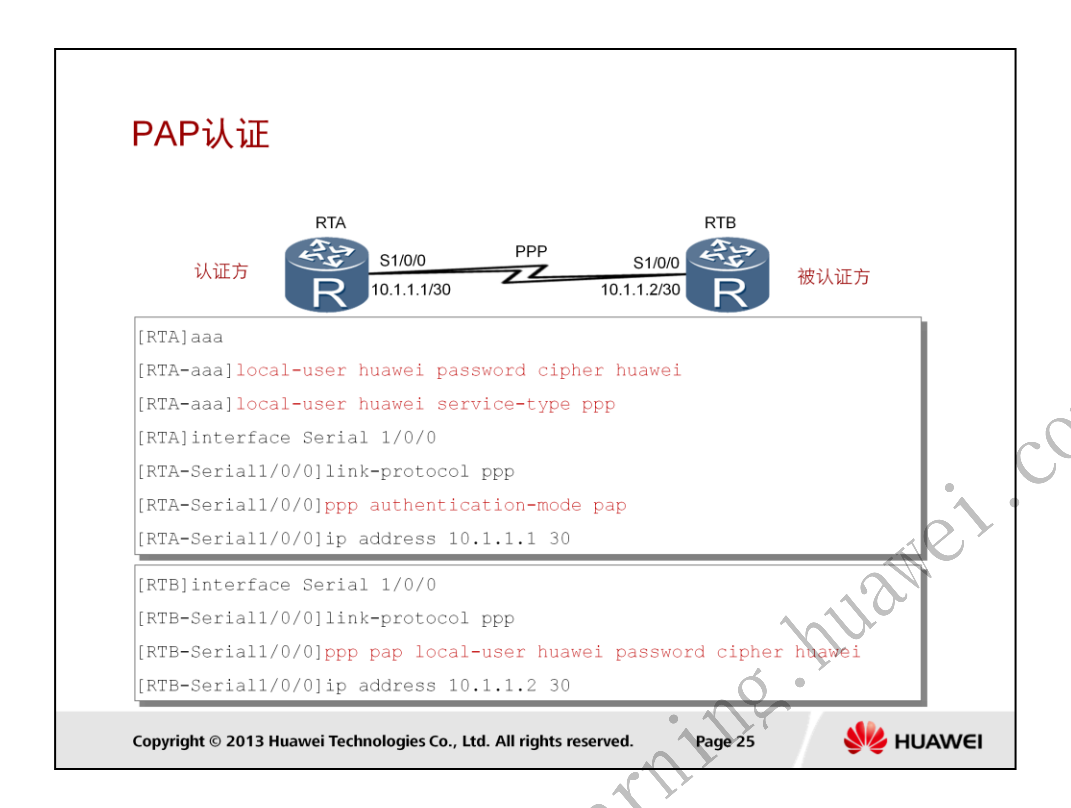
2. 每一端接收到此Configure-Request报文之后，检查其中的IP地址，如果IP地址是一个合法的单播IP地址，而且和本地配置的IP地址不同（没有IP冲突），则认为对端可以使用该地址，回应一个Configure-Ack报文。



两端动态协商IP地址的过程如下：

1. RTA向RTB发送一个Configure-Request报文，此报文中会包含一个IP地址0.0.0.0，表示向对端请求IP地址；
2. RTB收到上述Configure-Request报文后，认为其中包含的地址（0.0.0.0）不合法，使用Configure-Nak回应一个新的IP地址10.1.1.1；
3. RTA收到此Configure-Nak报文之后，更新本地IP地址，并重新发送一个Configure-Request报文，包含新的IP地址10.1.1.1；
4. RTB收到Configure-Request报文后，认为其中包含的IP地址为合法地址，回应一个Configure-Ack报文。

同时，RTB也要向RTA发送Configure-Request报文请求使用地址10.1.1.2，RTA认为此地址合法，回应Configure-Ack报文。



local-user huawei password cipher huawei命令用于创建一个本地用户，用户名为“huawei”，密码为“huawei”，关键字“cipher”表示密码信息在配置文件中被加密。

local-user huawei service-type ppp命令用于设置用户“huawei”为PPP用户。

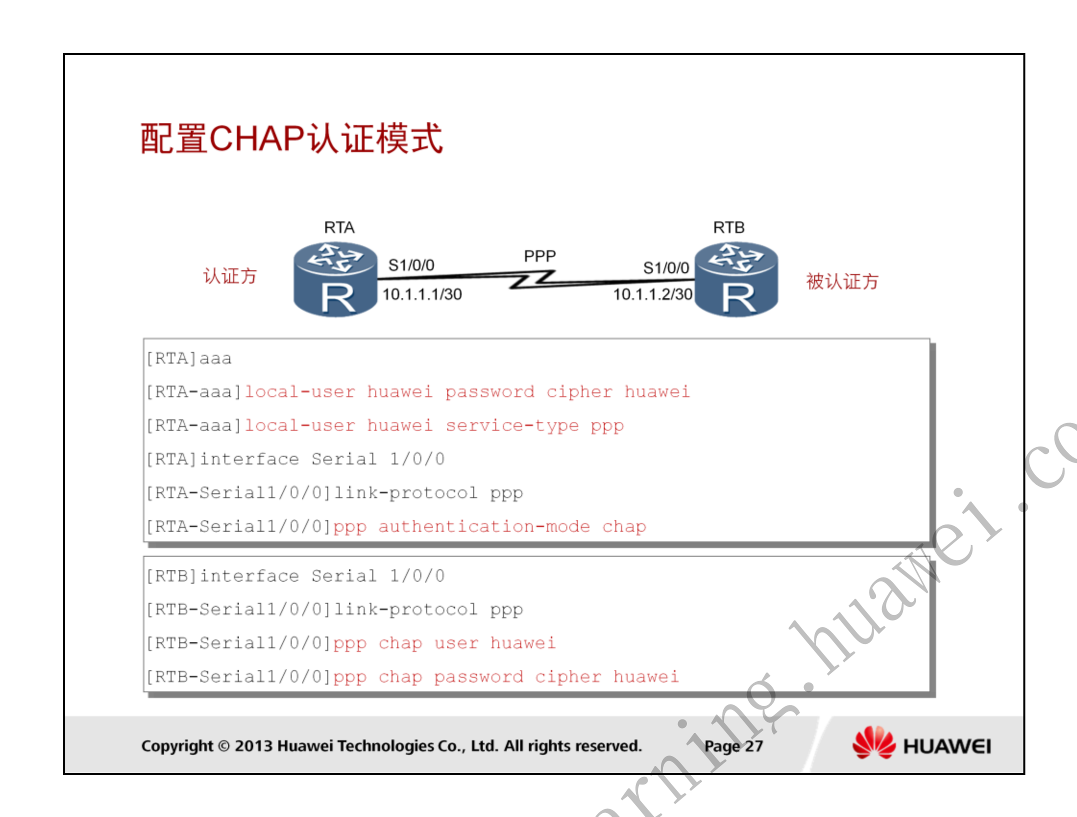
ppp authentication-mode pap命令用于在认证方开启PAP认证的功能，即要求对端使用PAP认证。

ppp pap local-user huawei password cipher huawei命令用于在被认证方配置PAP使用的用户名和密码信息。

配置验证

```
<RTB>debugging ppp pap all
Aug 20 2013 04:50:24.280.4+00:00 RTB PPP/7/debug2:
  PPP State Change:
      Serial1/0/0 PAP : Initial --> SendRequest
Aug 20 2013 04:50:24.290.3+00:00 RTB PPP/7/debug2:
  PPP State Change:
      Serial1/0/0 PAP : SendRequest --> ClientSuccess
……
```



local-user huawei password cipher huawei命令用于创建一个本地用户，用户名为“huawei”，密码为“huawei”；关键字“cipher”表示密码信息在配置文件中加密保存。

local-user huawei service-type ppp命令用于设置用户“huawei”为PPP用户。

ppp authentication-mode chap命令用于在认证方开启CHAP认证的功能，即要求对端使用CHAP认证。

ppp chap user huawei命令用于在被认证方设置CHAP使用的用户名为“huawei”。

ppp chap password cipher huawei命令用于在被认证方设置CHAP使用的密码为“huawei”。

配置验证

```
<RTB>debugging ppp chap all
Aug 20 2013 05:15:54.230.1+00:00 RTB PPP/7/debug2:
PPP State Change:
      Serial1/0/0 CHAP : Initial --> ListenChallenge
Aug 20 2013 05:15:54.230.7+00:00 RTB PPP/7/debug2:
  PPP State Change:
      Serial1/0/0 CHAP : ListenChallenge --> SendResponse
Aug 20 2013 05:15:54.250.3+00:00 RTB PPP/7/debug2:
  PPP State Change:
      Serial1/0/0 CHAP : SendResponse --> ClientSuccess
......
```






总结

- 发送端在发送Configure-Request之后，收到哪个消息才能表示PPP链路建立成功?
- CHAP认证方式需要交互几次报文?



1. 如果使用PPP作为链路层封装协议，需要建立PPP链路的两端设备都必须发送Configure-Request报文，当每个设备均已收到对端发来的Configure-Ack报文后，就表示链路的建立过程已成功完成。
2. CHAP认证协议为三次握手认证协议，需要交互三次报文来认证对方身份。


谢谢
www.huawei.com


帧中继原理与配置
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

帧中继FR（Frame Relay）协议工作在OSI参考模型的数据链路层，是一种主要应用在运营商网络中的广域网技术。当企业网络需要使用帧中继技术与运营商网络相连时，管理员也需要了解帧中继的工作原理，并具备相应的故障处理能力。

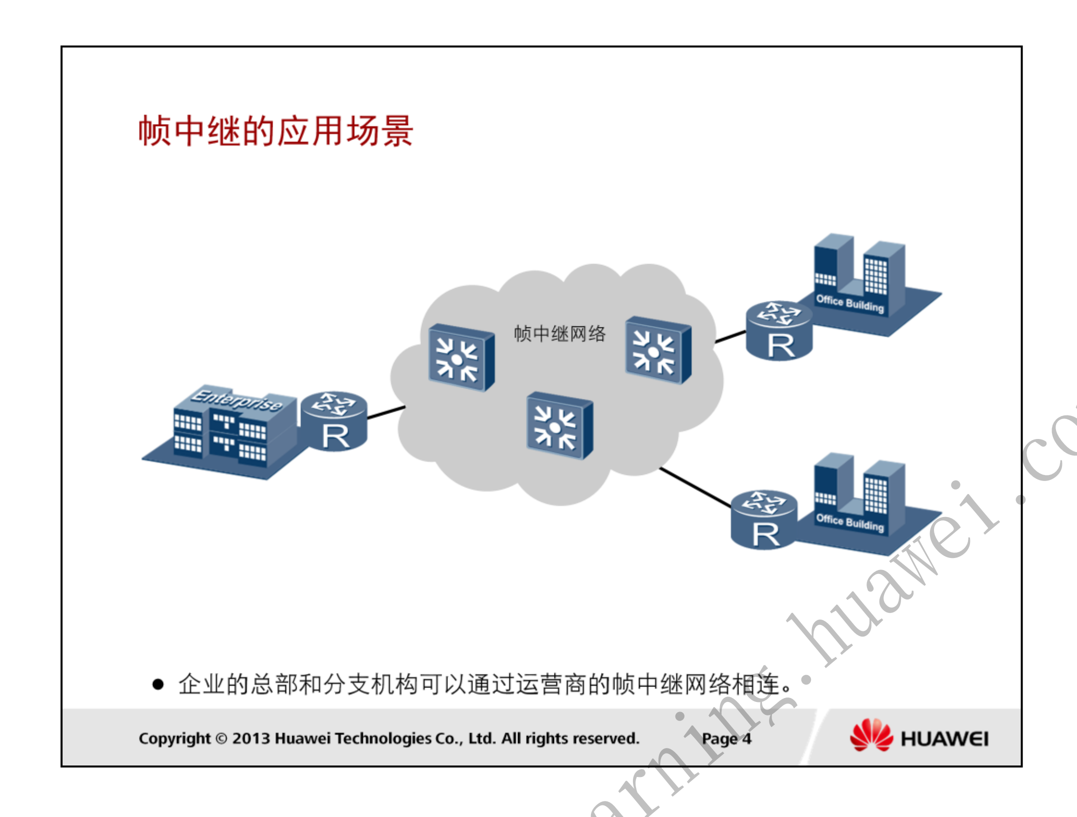




学习目标

学完本课程后，您应该能：

- 掌握帧中继的工作原理
- 掌握帧中继的基本配置

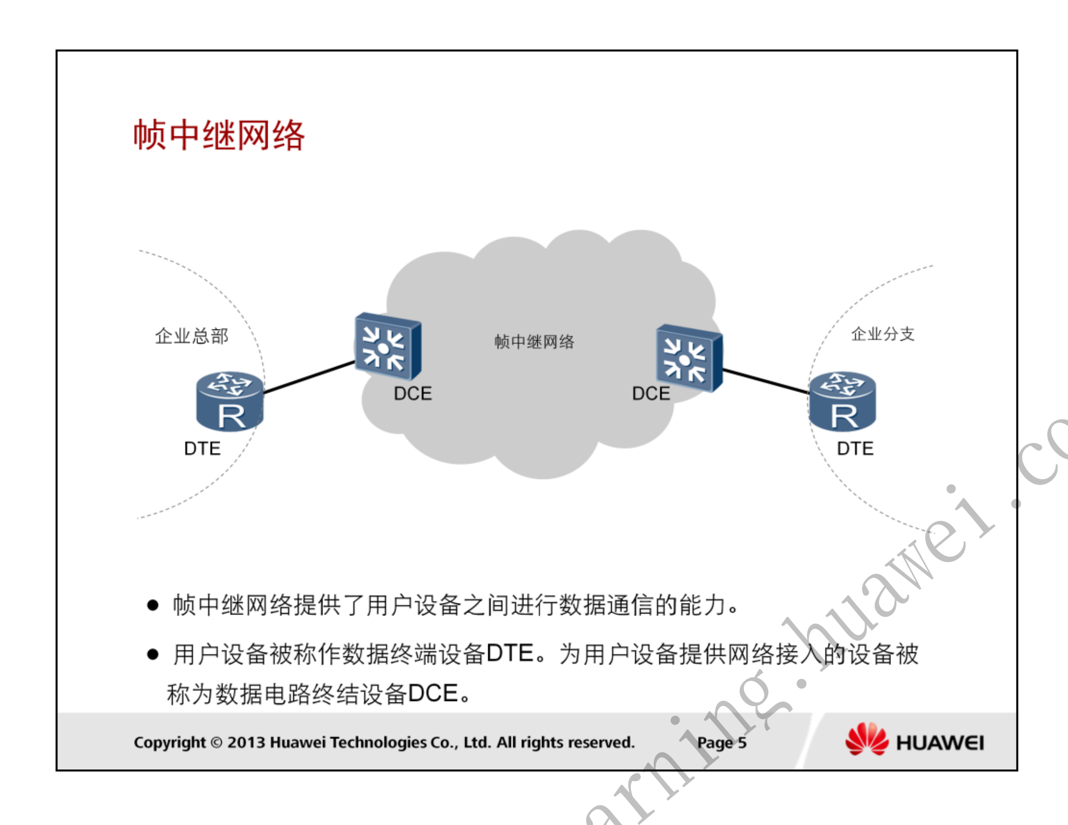


PPP、HDLC、X.25、FR、ATM都是常见的广域网技术。PPP和HDLC是一种点到点连接技术，而X.25、FR和ATM则属于分组交换技术。

X.25协议主要是描述如何在DTE和DCE之间建立虚电路、传输分组、建立链路、传输数据、拆除链路、拆除虚电路、同时进行差错控制、流量控量、情况统计等。

帧中继协议是一种简化了X.25的广域网协议，它在控制层面上提供了虚电路的管理、带宽管理和防止阻塞等功能。与传统的电路交换相比，它可以对物理电路实行统计时分复用，即在一个物理连接上可以复用多个逻辑连接，实现了带宽的复用和动态分配，有利于多用户、多速率的数据传输，充分利用了网络资源。

帧中继工作在OSI参考模型的数据链路层。与X.25协议相比，帧中继的一个显著的特点是将分组交换网中差错控制、确认重传、流量控制、拥塞避免等处理过程进行了简化，缩短了处理时间，提高了数字传输通道的利用率。新的技术诸如MPLS等的大量涌现，使得帧中继网络的部署逐渐减少。如果企业不得不使用运营商的帧中继网络服务，则企业管理员必须具备在企业边缘路由器上配置和维护帧中继的能力。



帧中继网提供了用户设备（如路由器和主机等）之间进行数据通信的能力。

用户设备被称作数据终端设备DTE（Data Terminal Equipment）。

为用户设备提供接入的设备，属于网络设备，被称为数据电路终结设备DCE（Data Circuit-terminating Equipment）。

虚电路

- 帧中继网络采用虚电路来连接网络两端的帧中继设备。
- 每条虚电路采用数据链路连接标识符DLCI来进行标识。

 Page 6 HUAWEI

帧中继是一种面向连接的技术，在通信之前必须建立连接，DTE之间建立的连接称为虚电路。帧中继虚电路有两种类型：PVC和SVC。

1. 永久虚电路PVC（Permanent Virtual Circuit）：是指给用户提供的固定的虚电路，该虚电路一旦建立，则永久生效，除非管理员手动删除。PVC一般用于两端之间频繁的、流量稳定的数据传输。目前在帧中继中使用最多的方式是永久虚电路方式。
2. 交换虚电路SVC（Switched Virtual Circuit）：是指通过协议自动分配的虚电路。在通信结束后，该虚电路会被自动取消 。一般突发性的数据传输多用SVC。

帧中继协议是一种统计复用协议，它能够在单一物理传输线路上提供多条虚电路，每条虚电路采用数据链路连接标识符DLCI（Data Link Connection Identifier）来进行标识。DLCI只在本地接口和与之直接相连的对端接口有效，不具有全局有效性，即在帧中继网络中，不同的物理接口上相同的DLCI并不表示是同一个虚电路。用户可用的DLCI的取值范围是16～1022，其中1007到1022是保留DLCI。

LMI协商过程

DCE

DLCI 100

DTE

S1/0/0

10.1.1.1/24

状态查询消息

状态应答消息

决定链路状态和PVC状态

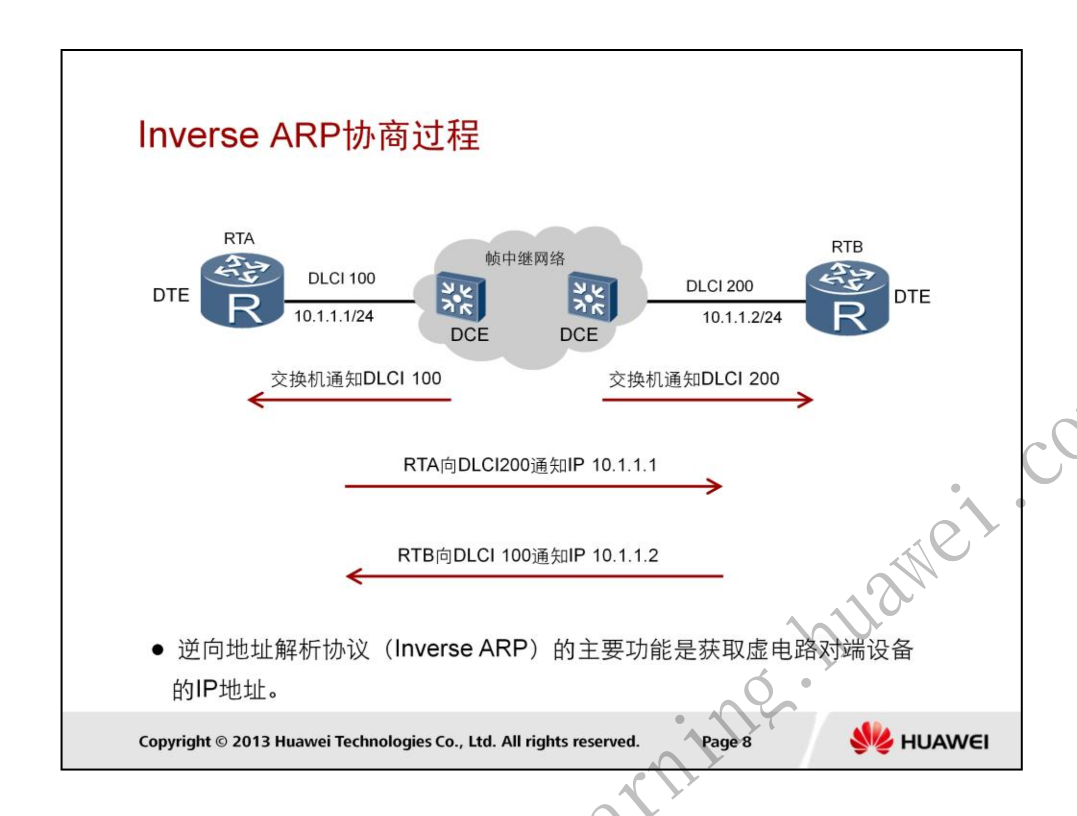
- 本地管理接口LMI协议通过状态查询报文和状态应答报文维护帧中继的链路状态和PVC状态。

 Page 7 HUAWEI

PVC方式下，不管是网络设备还是用户设备都需要知道PVC的当前状态。监控PVC状态的协议叫本地管理接口LMI（Local Management Interface）。LMI协议通过状态查询报文和状态应答报文维护帧中继的链路状态和PVC状态。LMI用于管理PVC，包括PVC的增加、删除，PVC链路完整性检测，PVC的状态等。

LMI协商过程如下：

1. DTE端定时发送状态查询消息（Status Enquiry）。
2. DCE端收到查询消息后，用状态消息（Status）应答状态查询消息。
3. DTE解析收到的应答消息，以了解链路状态和PVC状态。
4. 当两端设备LMI协商报文收发正确的情况下，PVC状态将变为Active状态。



逆向地址解析协议InARP（Inverse ARP）的主要功能是获取每条虚电路连接的对端设备的IP地址。如果知道了某条虚电路连接的对端设备的IP地址，在本地就可以生成对端IP地址与本地DLCI的映射，从而避免手工配置地址映射。

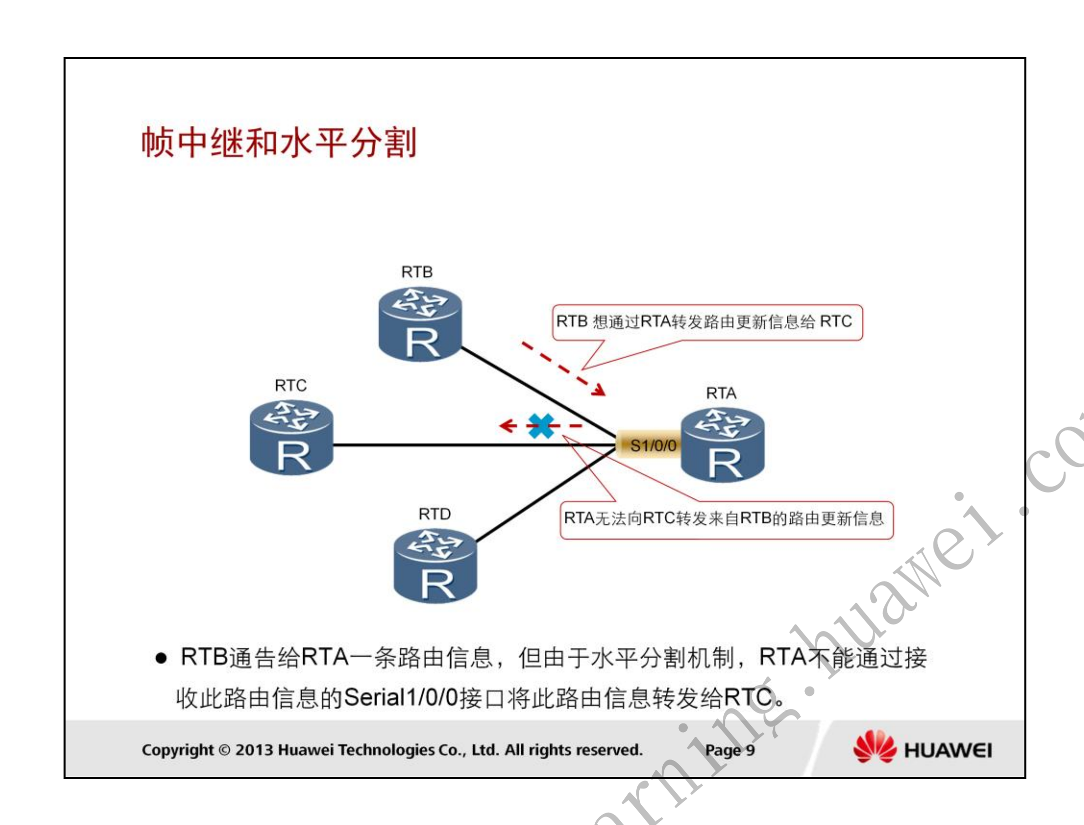
当帧中继LMI协商通过，PVC状态变为Active后，就会开始InARP协商过程。

InARP协商过程如下:

1. 如果本地接口上已配置了IP地址，那么设备就会在该虚电路上发送Inverse ARP请求报文给对端设备。该请求报文包含有本地的IP地址。
2. 对端设备收到该请求后，可以获得本端设备的IP地址，从而生成地址映射，并发送Inverse ARP响应报文进行响应。
3. 本端收到Inverse ARP响应报文后，解析报文中的对端IP地址，也生成地址映射。

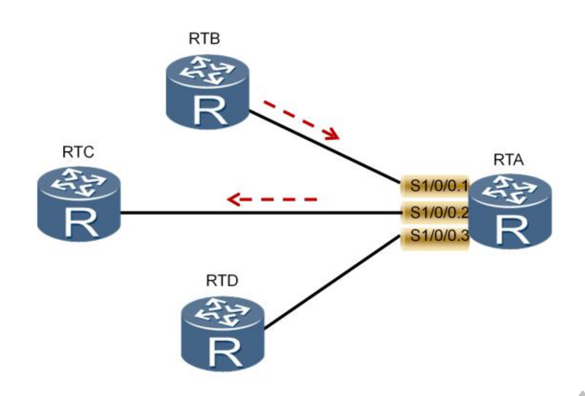
本例中，RTA会生成地址映射（10.1.1.2<--->100），RTB会生成地址映射（10.1.1.1<--->200）。

经过LMI和InARP协商后，帧中继接口的协议状态将变为Up状态，并且生成了对端IP地址的映射，这样PVC上就可以承载IP报文了。



为了减少路由环路的产生，路由协议的水平分割机制不允许路由器把从一个接口接收到的路由更新信息再从该接口发送出去。水平分割机制虽然可以减少路由环路的产生，但有时也会影响网络的正常通信。例如，本例中，RTB想通过RTA转发路由信息给RTC，但由于开启了水平分割，RTA无法通过S1/0/0接口向RTC转发RTB的路由信息。

帧中继子接口



- 在一个物理接口上配置多个子接口，每个子接口使用一条虚电路连接到对端的路由器，这样就可以解决水平分割带来的问题。

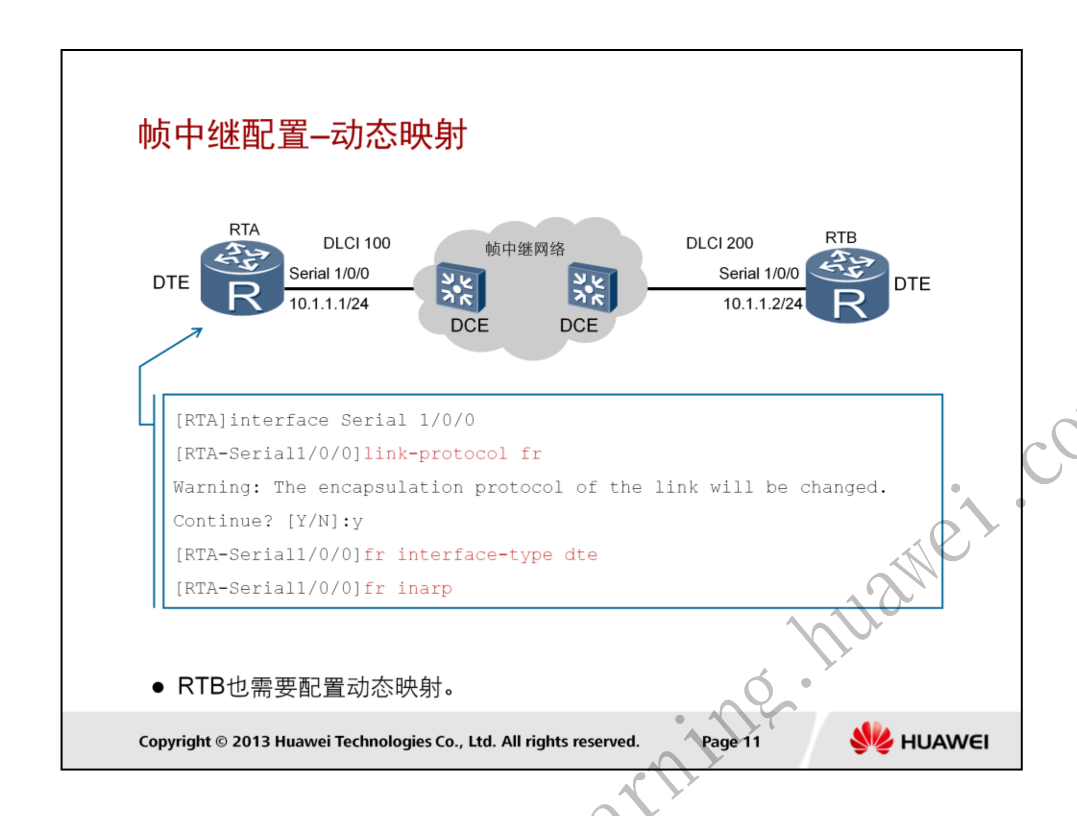
 Page 10 

子接口可以解决水平分割带来的问题，一个物理接口可以包含多个逻辑子接口，每一个子接口使用一个或多个DLCI连接到对端的路由器。本例中，RTA通过子接口S1/0/0.1接收到来自RTB的路由信息，然后将此信息通过子接口S1/0/0.2转发给RTC。

帧中继的子接口分为两种类型。

点到点（point-to-point）子接口：用于连接单个远端设备。一个子接口只配一条PVC，不用配置静态地址映射就可以唯一地确定对端设备。

点到多点（point-to-multipoint）子接口：用于连接多个远端设备。一个子接口上配置多条PVC，每条PVC都和它相连的远端协议地址建立地址映射，这样不同的PVC就可以到达不同的远端设备。



link-protocol fr命令用来指定接口链路层协议为帧中继协议。当封装帧中继协议时，缺省情况下，帧的封装格式为IETF。

fr interface-type { dce | dte }命令用来设置帧中继接口类型。缺省情况下，帧中继接口类型为DTE。在实际应用中，DTE接口只能和DCE接口直连。如果把设备用作帧中继交换机，则帧中继接口类型应该为DCE。

fr inarp命令用来使能帧中继逆向地址解析功能。缺省情况下，该功能已被使能。

配置验证

```
[RTA]display fr pvc-info
PVC statistics for interface Serial1/0/0 (DTE, physical UP)
    DLCI = 100, USAGE = UNUSED (00000000), Serial1/0/0
    create time = 2013/08/20 09:02:33, status = ACTIVE
    InARP = Enable, PVC-GROUP = NONE
    in packets = 6, in bytes = 11230
    out packets = 7, out bytes = 500
```

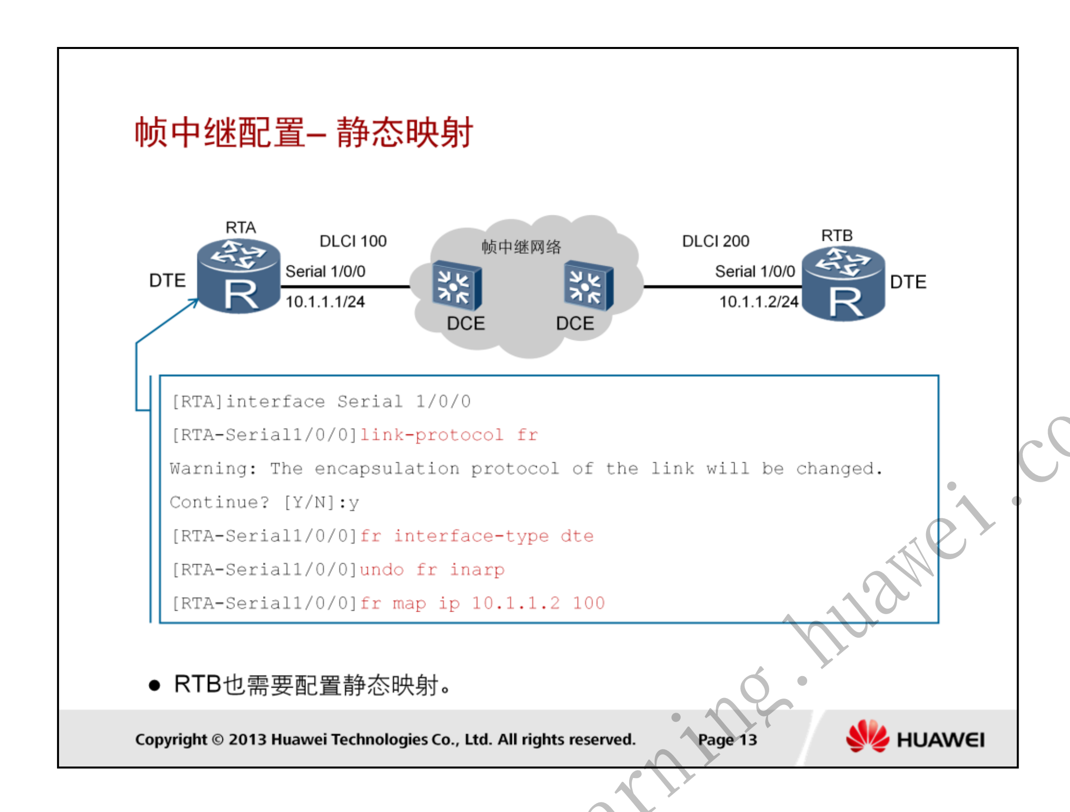
```
[RTA]display fr map-info
Map Statistics for interface Serial1/0/0 (DTE)
  DLCI = 100, IP INARP 10.1.1.2, Serial1/0/0
    create time = 2013/08/20 12:51:46, status = ACTIVE
    encapsulation = ietf, vlink = 2, broadcast
```

 Page 12



display fr pvc-info命令可以用来查看帧中继虚电路的配置情况和统计信息。

在显示信息中，DLCI表示虚电路的标识符。USAGE表示此虚电路的来源。LOCAL表示PVC是本地配置的，如果是UNUSED，则表示PVC是从DCE侧学习来的。status表示虚电路状态。可能的取值有：active：表示虚电路处于激活状态。inactive：表示虚电路处于未激活状态。InARP表示是否使能InARP功能。



fr map ip [*destination-address* [*mask*] *dlci-number*]命令用来配置一个目的IP地址和指定DLCI的静态映射。

如果DCE侧设备配置静态地址映射，DTE侧启动动态地址映射功能，则DTE侧不需要再配置静态地址映射也可实现两端互通。反之，如果DCE配置动态地址映射，DTE配置静态地址映射，则不能实现互通。

fr map ip [*destination-address* [*mask*] *dlci-number*] **broadcast**命令用来配置该映射上可以发送广播报文。

配置验证

```
[RTA]display fr pvc-info
   DLCI = 100, USAGE = LOCAL (00000100), Serial1/0/0
   create time = 2013/08/20 09:02:59, status = ACTIVE
   InARP = Disable, PVC-GROUP = NONE
   in packets = 10, in bytes = 253403
   out packets = 11, out bytes = 620
```

```
[RTA]display fr map-info
Map Statistics for interface Serial1/0/0 (DTE)
  DLCI = 100, IP 10.1.1.2, Serial1/0/0
    create time = 2013/08/20 12:45:48, status = ACTIVE
    encapsulation = ietf, vlink = 2
```

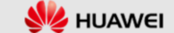



display fr map-info命令用来显示帧中继地址映射表，可以显示当前设备上目的IP地址和DLCI的映射关系。status表示地址映射的状态。



总结

- 帧中继网络中DLCI的作用是什么?
- Inverse ARP在帧中继中有什么作用?



1. DLCI是数据链路连接标识，每条虚电路用它来进行标识。DLCI只在本地接口和与之直接相连的对端接口有效，不具有全局有效性，即在帧中继网络中，不同物理接口上相同的DLCI并不表示同一个虚连接。
2. 逆向地址解析协议Inverse ARP可以用来获取每条虚电路连接的对端设备的IP地址，然后在本地形成对端IP地址与DLCI的映射关系。


谢谢
www.huawei.com


PPPoE原理和配置
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

数字用户线路DSL(Digital Subscriber Line)是以电话线为传输介质的传输技术，人们通常把所有的DSL技术统称为xDSL，x代表不同种类的数字用户线路技术。目前比较流行的宽带接入方式为ADSL，ADSL是非对称DSL技术，使用的是PPPoE（PPP over Ethernet）协议。

PPPoE协议通过在以太网上提供点到点的连接，建立PPP会话，使得以太网中的主机能够连接到远端的宽带接入服务器上。PPPoE具有适用范围广、安全性高、计费方便等特点。

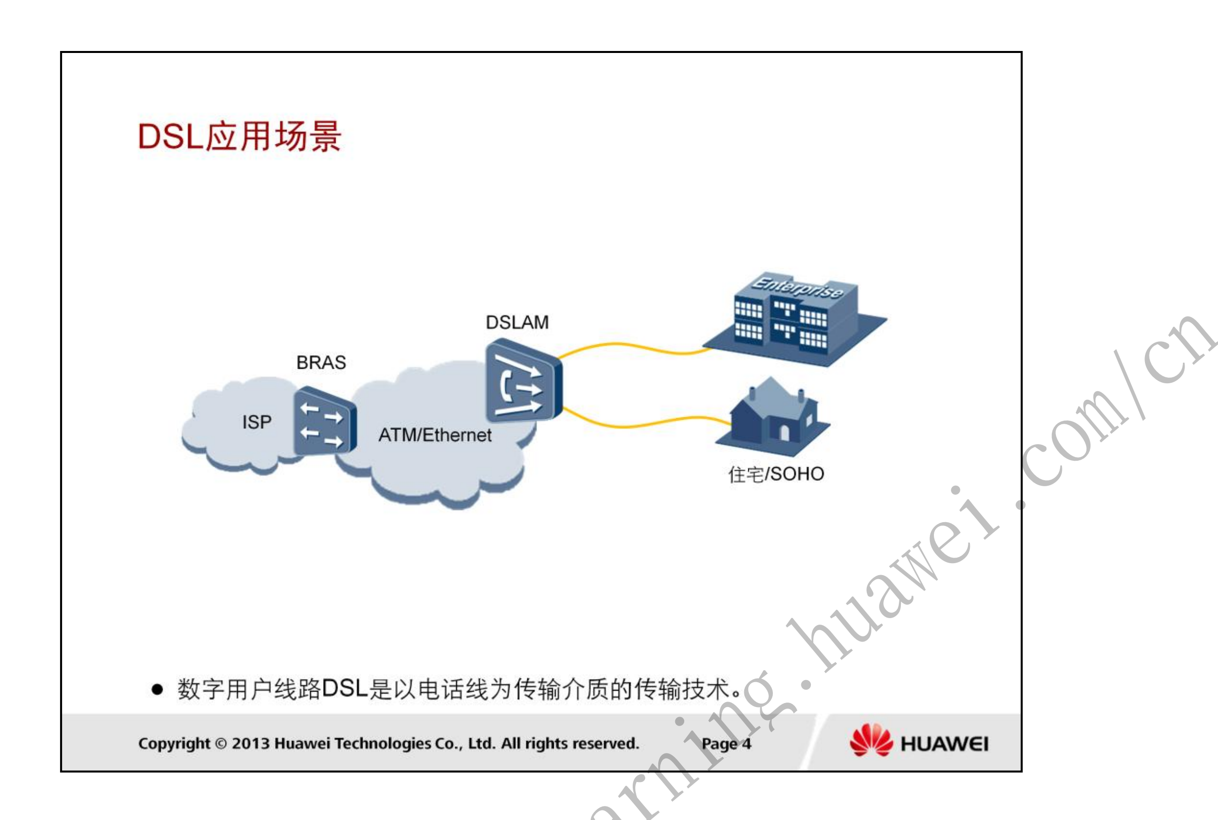




学习目标

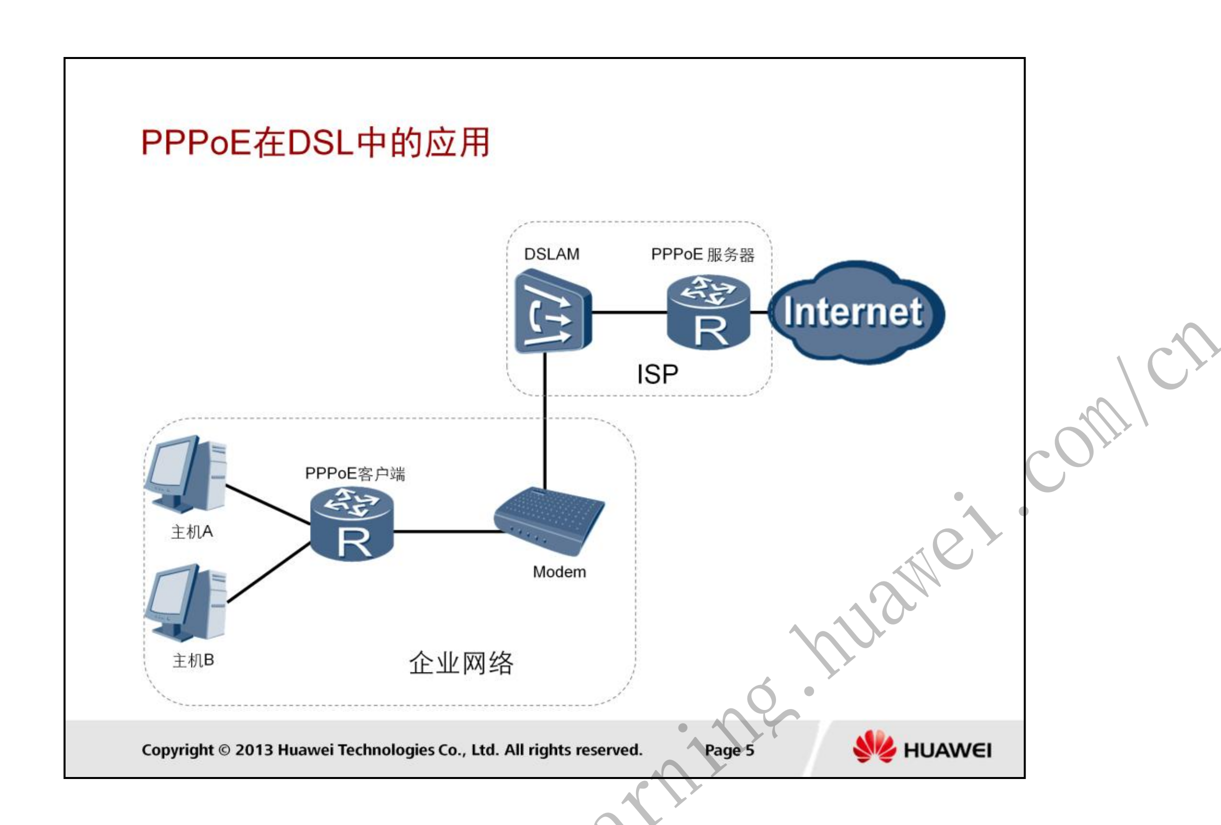
学完本课程后，您应该能：

- 掌握PPPoE连接协商过程
- 掌握PPPoE的配置



DSL是一种利用现有电话网络实现数据通信的宽带技术。在使用DSL接入网络时，用户侧会安装调制解调器，然后通过现有的电话线与数字用户线路接入复用器（DSLAM）相连。DSLAM是各种DSL系统的局端设备，属于最后一公里接入设备。

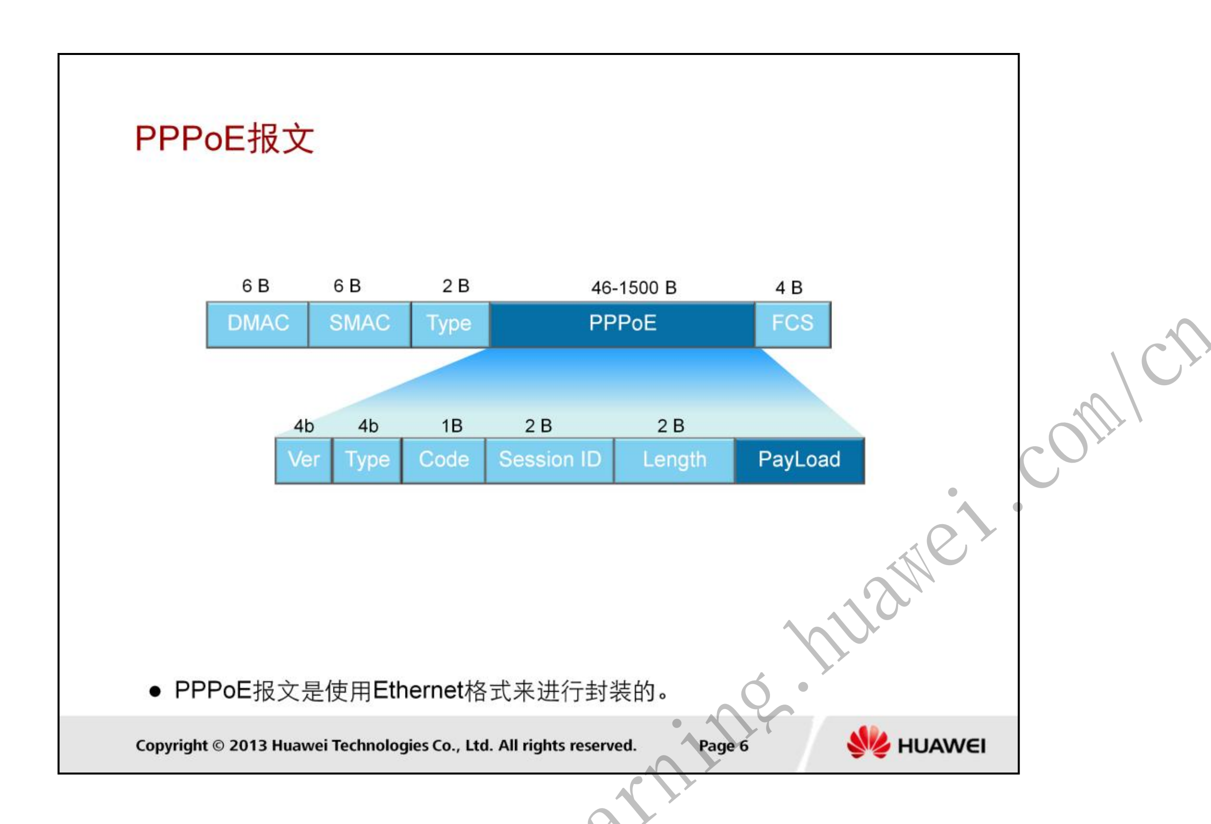
然后，DSLAM通过高速ATM网络或者以太网将用户的数据流量转发给宽带远程接入服务器（BRAS）。BRAS是面向宽带网络应用的接入网关，位于骨干网的边缘层。



运营商希望通过同一台接入设备来连接远程的多个主机，同时接入设备能够提供访问控制和计费功能。在众多的接入技术中，把多个主机连接到接入设备的最经济的方法就是以太网，而PPP协议可以提供良好的访问控制和计费功能，于是产生了在以太网上传输PPP报文的技术，即PPPoE。

PPPoE利用以太网将大量主机组成网络，通过一个远端接入设备连入因特网，并运用PPP协议对接入的每个主机进行控制，具有适用范围广、安全性高、计费方便的特点。

PPPoE技术解决了用户上网收费等实际应用问题，得到了宽带接入运营商的认可并被广泛应用。



PPPoE报文是使用Ethernet格式进行封装的，Ethernet中各字段解释如下：

1. DMAC：表示目的设备的MAC地址，通常为以太网单播目的地址或者以太网广播地址（0xFFFFFFFF）。
2. SMAC：表示源设备的以太网MAC地址。
3. Type：表示协议类型字段，当值为0x8863时表示承载的是PPPoE发现阶段的报文。当值为0x8864时表示承载的是PPPoE会话阶段的报文。

PPPoE字段中的各个字段解释如下：

1. VER：表示PPPoE版本号，值为0x01。
2. Type：表示类型，值为0x01。
3. Code：表示PPPoE报文类型，不同取值标识不同的PPPoE报文类型。
4. PPPoE会话ID，与以太网SMAC和DMAC一起定义了一个PPPoE会话。
5. Length：表示PPPoE报文的Payload长度，不包括以太网头部和PPPoE头部的长度。

PPPoE会话建立过程

阶段	描述
发现阶段	获取对方以太网地址，以及确定唯一的PPPoE会话。
会话阶段	包含两部分：PPP协商阶段和PPP报文传输阶段。
会话终结阶段	会话建立以后的任意时刻，发送报文结束PPPoE会话



PPPoE可分为三个阶段，即发现阶段、会话阶段和会话终结阶段。

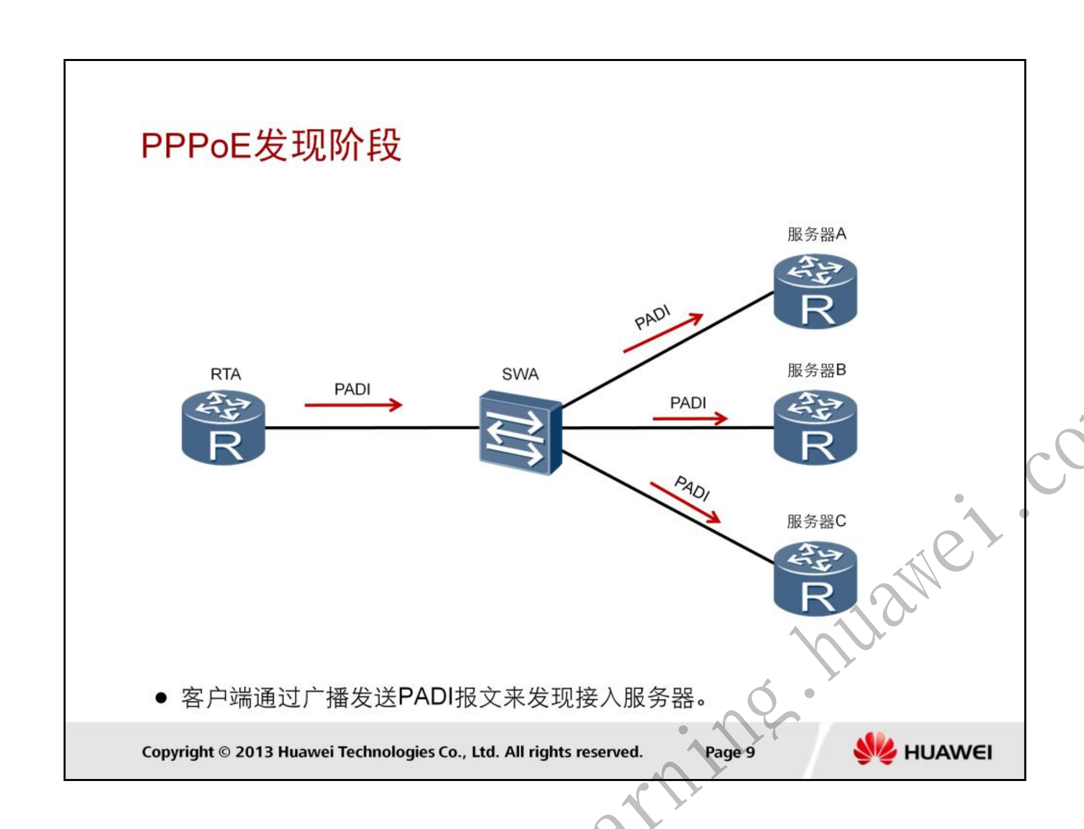
PPPoE协议报文

类型	描述
PADI	PPPoE发现初始报文
PADO	PPPoE发现提供报文
PADR	PPPoE发现请求报文
PADS	PPPoE发现会话确认报文
PADT	PPPoE发现终止报文

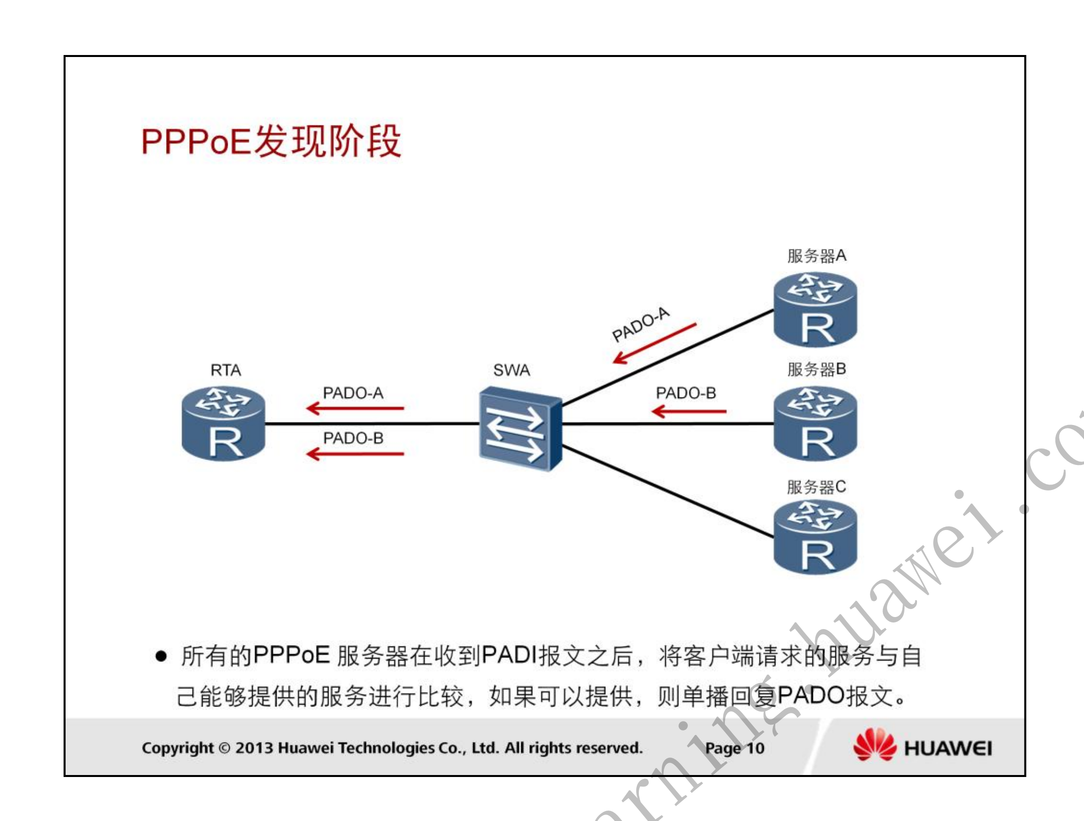
- PPPoE通过这五种类型的报文来建立和终结PPPoE会话。



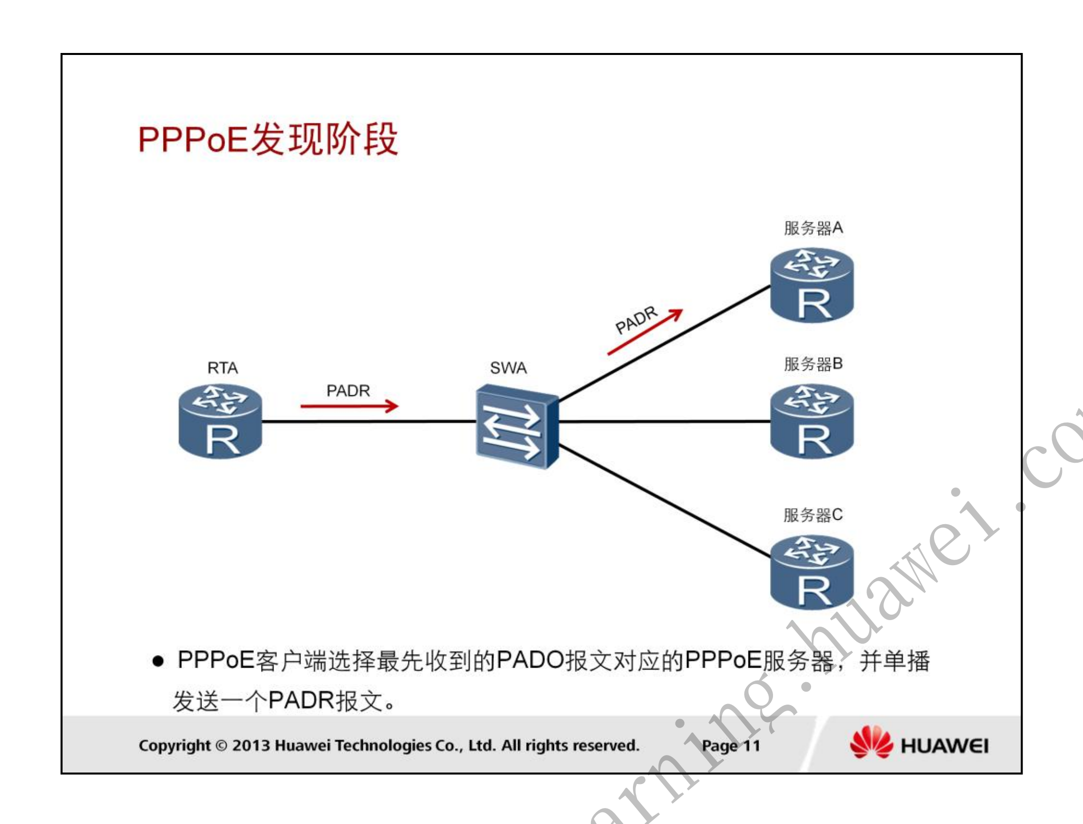
1. PADI（PPPoE Active Discovery Initiation）报文：用户主机发起的PPPoE服务器探测报文，目的MAC地址为广播地址。
2. PADO（PPPoE Active Discovery Offer）报文：PPPoE服务器收到PADI报文之后的回应报文，目的MAC地址为客户端主机的MAC地址。
3. PADR（PPPoE Active Discovery Request）报文：用户主机收到PPPoE服务器回应的PADO报文后，单播发起的请求报文，目的地址为此用户选定的那个PPPoE服务器的MAC地址。
4. PADS（PPPoE Active Discovery Session Configuration）报文：PPPoE服务器分配一个唯一的会话进程ID,并通过PADS报文发送给主机。
5. PADT（PPPoE Active Discovery Terminate）报文：当用户或者服务器需要终止会话时,可以发送这种PADT报文。



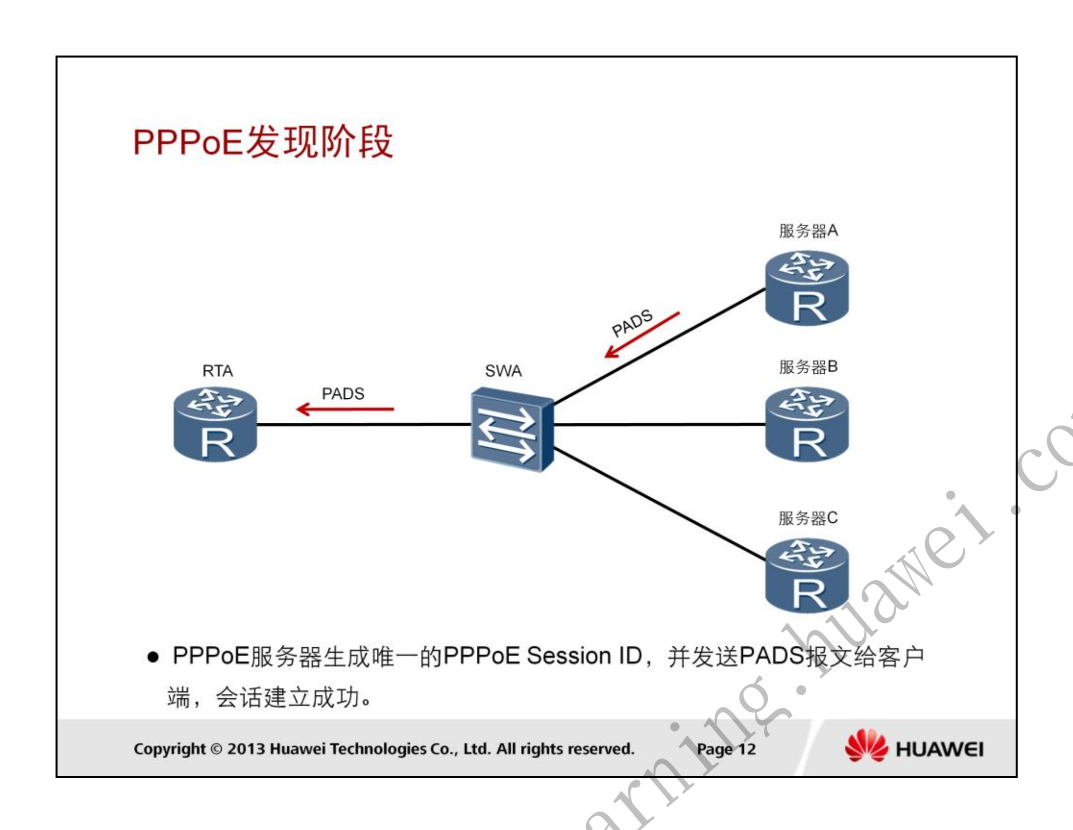
在发现阶段，PPPoE客户端在本地以太网中广播一个PADI报文，此PADI报文中包含了客户端需要的服务信息。在PADI报文中，目的MAC地址是一个广播地址，Code字段为0x09，Session ID字段为0x0000。所有PPPoE服务器收到PADI报文之后，会将报文中所请求的服务与自己能够提供的服务进行比较。



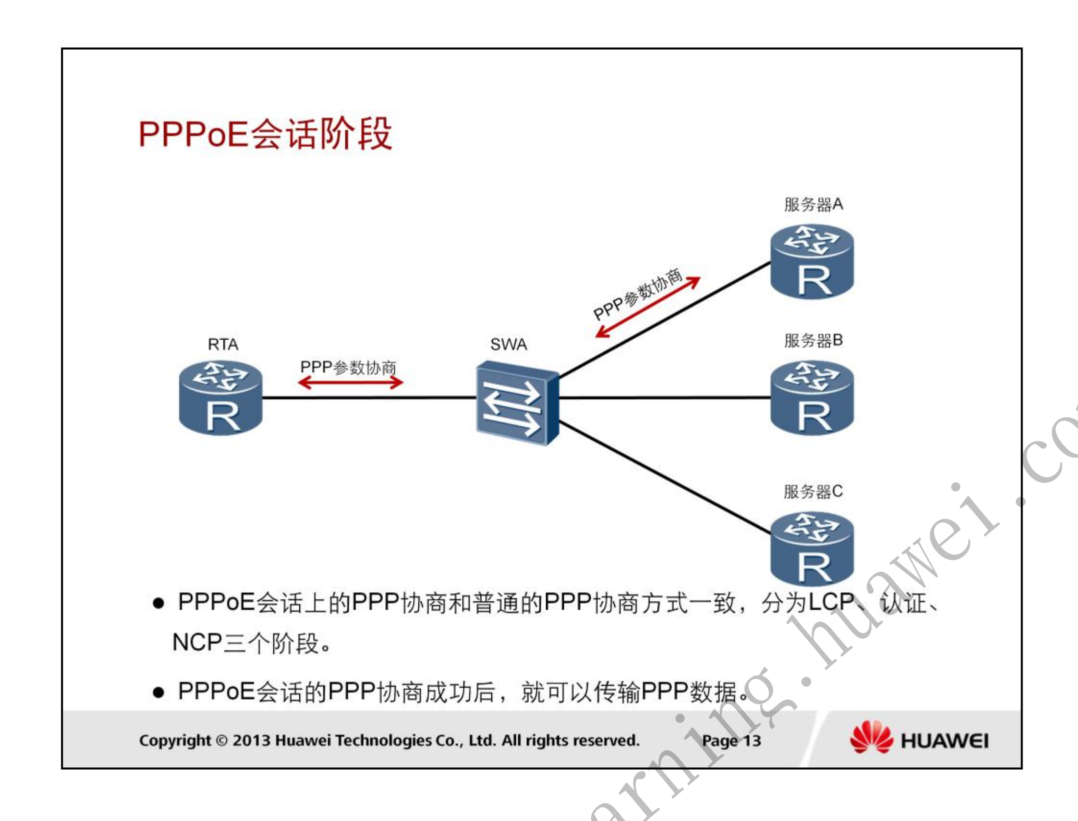
如果服务器可以提供客户端请求的服务，就会回复一个PADO报文。客户端（RTA）可能会收到多个PPPoE服务器发送的PADO报文。在PADO报文中，目的地址是发送PADI报文的客户端MAC地址，Code字段为0x07，Session ID字段为0x0000。



因为PPPoE客户端是以广播的形式发送PADI报文，所以客户端可能会收到多个PADO报文。在接收到的所有PADO报文中，PPPoE客户端选择最先收到的PADO报文对应的PPPoE服务器，并发送一个PADR报文给这个服务器。在PADR报文中，目的地址是选中的服务器的MAC地址，Code字段为0x19，Session ID字段为0x0000。

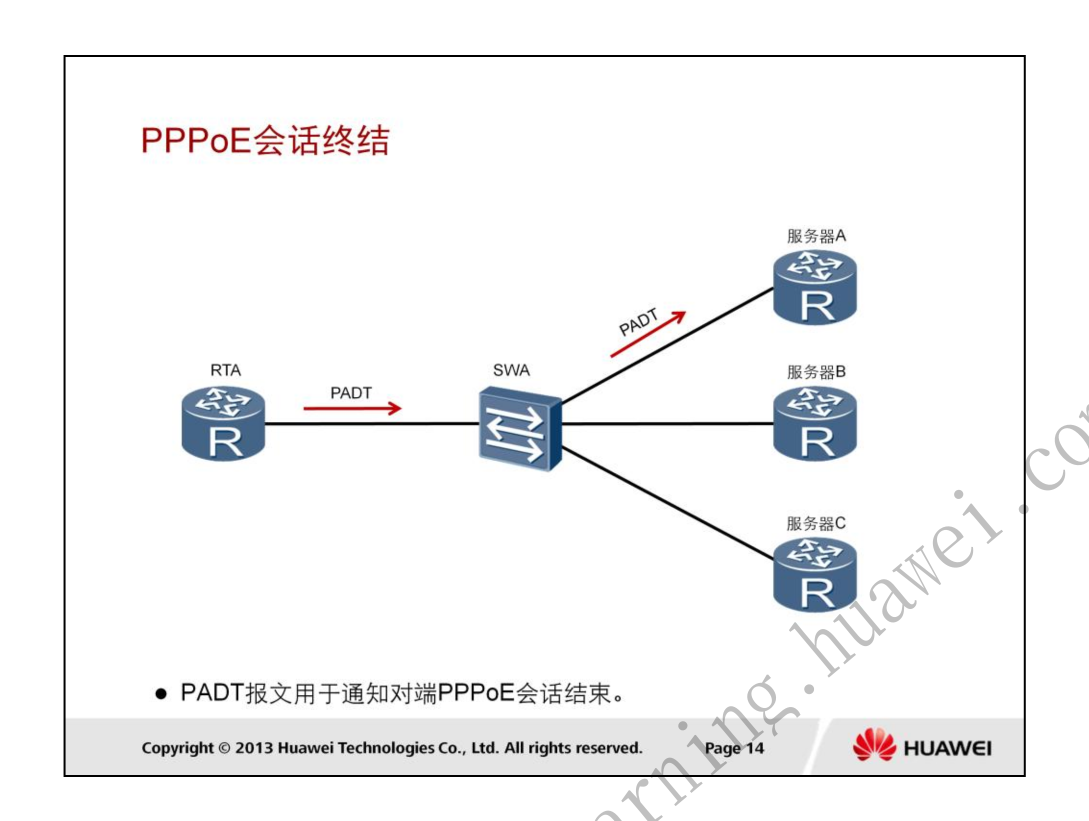


PPPoE服务器收到PADR报文后，会生成一个唯一的Session ID来标识和PPPoE客户端的会话，并通过一个PADS报文把Session ID发送给PPPoE客户端。在PADS报文中，目的地址是PPPoE客户端的MAC地址，Code字段为0x65，Session ID字段是PPPoE服务器为本PPPoE会话产生的Session ID。会话建立成功后，PPPoE客户端和服务器进入PPPoE会话阶段。



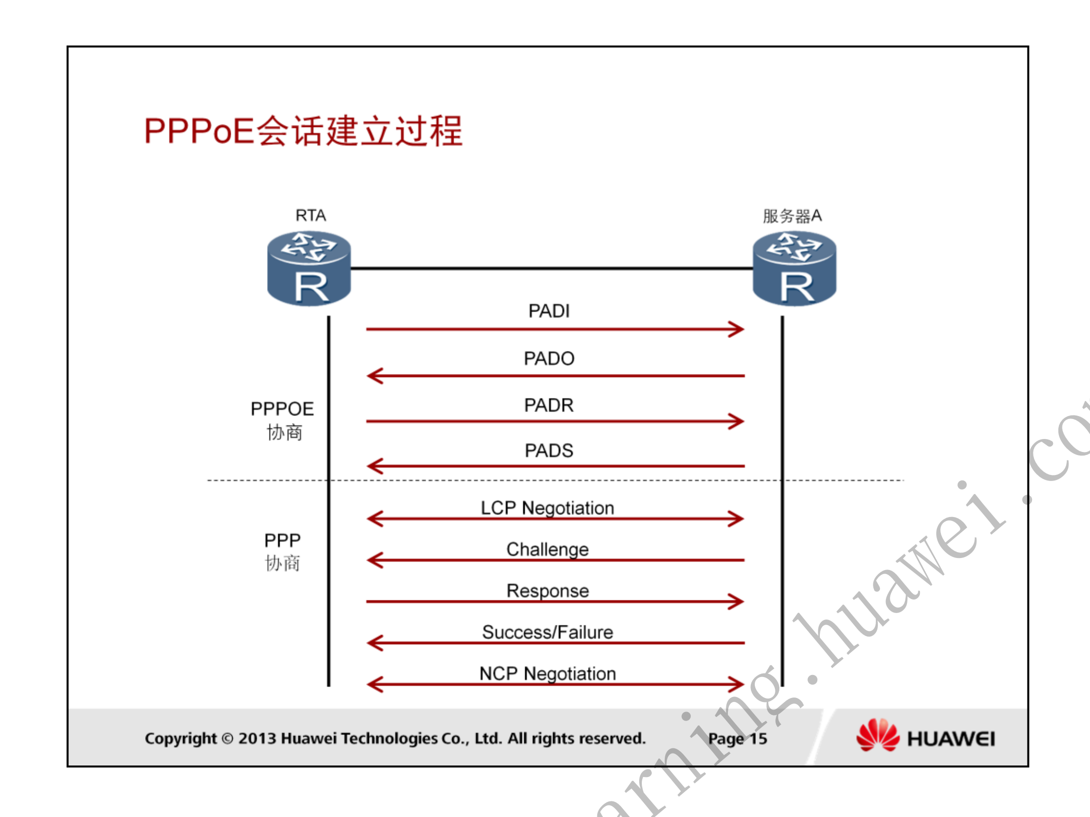
PPPoE会话阶段可分为两部分：PPP协商阶段和PPP报文传输阶段。

1. PPPoE Session上的PPP协商和普通的PPP协商方式一致，分为LCP、认证、NCP三个阶段。LCP阶段主要完成建立、配置和检测数据链路连接。LCP协商成功后，开始进行认证，认证协议类型由LCP协商结果决定。认证成功后，PPP进入NCP阶段，NCP是一个协议族，用于配置不同的网络层协议，常用的是IP控制协议（IPCP），它负责配置用户的IP地址和DNS服务器地址等。
2. PPPoE Session的PPP协商成功后，就可以承载PPP数据报文。在这一阶段传输的数据包中必须包含在发现阶段确定的Session ID并保持不变。

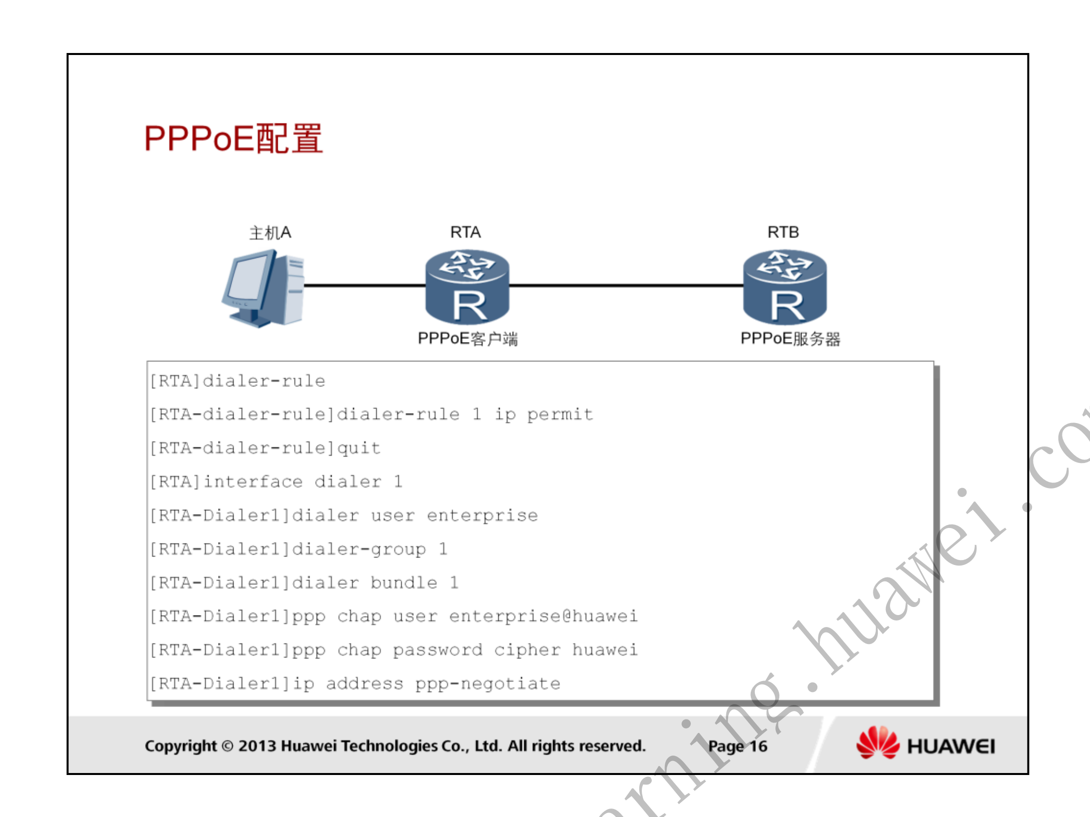


当PPPOE客户端希望关闭连接时，可以向PPPOE服务器端发送一个PADT报文。同样，如果PPPOE服务器端希望关闭连接时，也可以向PPPOE客户端发送一个PADT报文，此报文用于关闭连接。

在PADT报文中，目的MAC地址为单播地址，Session ID为希望关闭的连接的Session ID。一旦收到一个PADT报文之后，连接随即关闭。



1. 用户客户端向服务器发送一个PADI报文，开始PPPOE接入。
2. 服务器向客户端发送PADO报文。
3. 客户端根据回应，发起PADR请求给服务器。
4. 服务器产生一个Session ID，通过PADS发给客户端。
5. 客户端和服务器之间进行PPP的LCP协商，建立链路层通信。同时，协商使用CHAP认证方式。
6. 服务器通过Challenge报文发送给认证客户端，提供一个128bit的Challenge。
7. 客户端收到Challenge报文后，并将密码和Challenge做MD5算法运算后，在Response回应报文中把结果发送给服务器。
8. 服务器根据用户发送的信息判断用户是否合法，然后回应认证成功/失败报文，将认证结果返回给客户端。
9. 进行NCP（如IPCP）协商，通过服务器获取到规划的IP地址等参数。



PPPoE客户端配置包括三个步骤。

首先需要配置一个拨号接口。

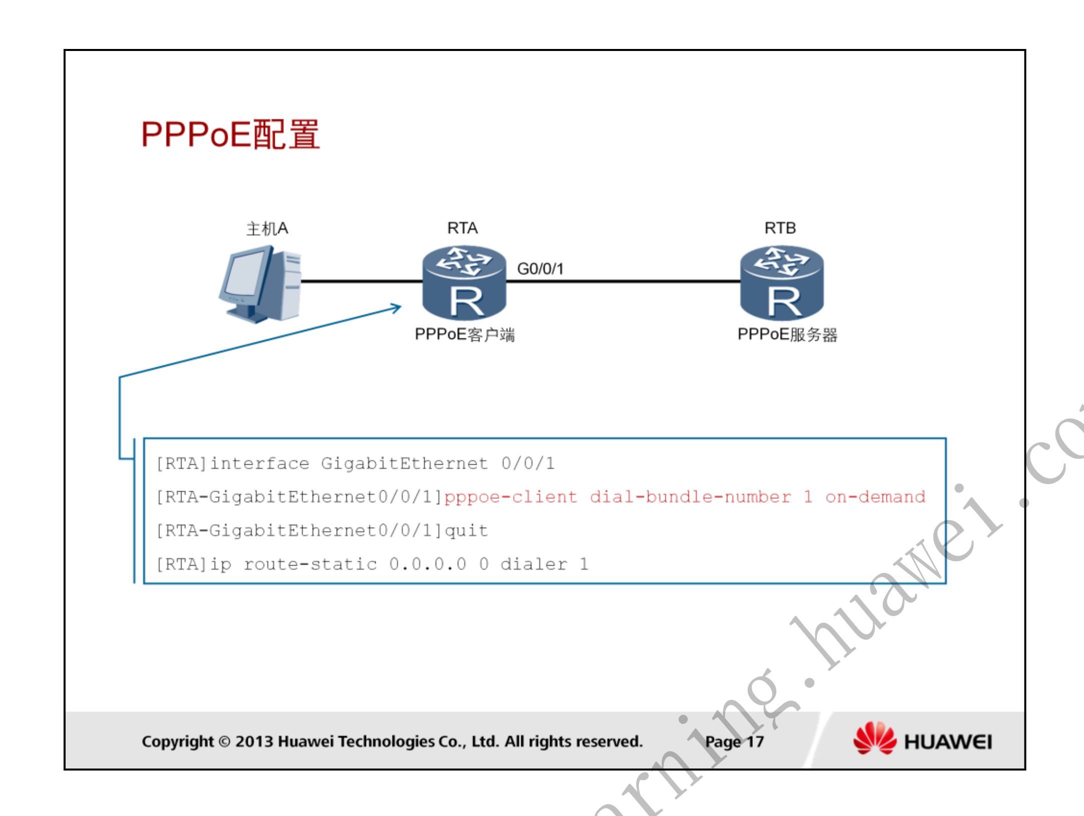
dialer-rule命令用于进入Dialer-rule视图，在该视图下，可以通过拨号规则来配置发起PPPoE会话的条件。

interface dialer *number*命令用来创建并进入Dialer接口。

dialer user *user-name*命令用于配置对端用户名，这个用户名必须与对端服务器上的PPP用户名相同。

dialer-group *group-number*命令用来将接口置于一个拨号访问组。

dialer bundle *number*命令用来指定Dialer接口使用的Dialer bundle。设备通过Dialer bundle将物理接口与拨号接口关联起来。



第二个步骤是在接口上将Dialer Bundle和接口绑定：

pppoe-client dial-bundle-number *number*命令来实现Dialer Bundle和物理接口的绑定，用来指定PPPoE会话对应的Dialer Bundle，其中*number*是与PPPoE会话相对应的Dialer Bundle编号。**on-demand**表示PPPoE会话工作在按需拨号模式。AR2200支持报文触发方式的按需拨号。目前ARG3系列路由器支持的按需拨号方式为报文触发方式，即当物理线路Up后，设备不会立即发起PPPoE呼叫，只有当有数据需要传送时，设备才会发起PPPoE呼叫，建立PPPoE会话。

第三个步骤是配置一条缺省静态路由，该路由允许在路由表中没有相应匹配表项的流量都能通过拨号接口发起PPPoE会话。

配置验证

```
<RTA>display interface Dialer 1
Dialer1 current state: UP
Line protocol current state: UP (spoofing)
Description: HUAWEI, AR Series, Dialer1 Interface
Route Port, The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is negotiated, 192.168.10.254/32
Link layer protocol is PPP
LCP initial
Physical is Dialer
Bound to Dialer1:0:
Dialer1:0 current state : UP
Line protocol current state : UP

Link layer protocol is PPP
LCP opened, IPCP opened
```


display interface dialer[*number*]命令用于查看拨号接口的配置，便于定位拨号接口的故障。

LCP opened, IPCP opened表示链路的状态完全正常。

配置验证

```
[RTA]display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf          Client-MAC    Server-MAC    State
0    1       1       GE0/0/1       54899876830c  000000000000  IDLE
```

```
[RTA]display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf          Client-MAC    Server-MAC    State
1    1       1       GE0/0/1       00e0fc0308f6  00e0fc036781  UP
```


Page 19


display pppoe-client session summary命令用于查看PPPoE客户端的PPPoE会话状态和统计信息。

本节给出了两个例子来说明不同的PPPoE会话状态。

ID表示PPPoE会话ID，Bundle ID和Dialer ID的值与拨号参数配置有关。

Intf表示客户端侧协商时的物理接口。

State表示PPPoE会话的状态，包括以下四种：

1. **DLE**表示当前会话状态为空闲。
2. **PADI**表示PPPoE会话处于发现阶段，并已经发送PADI报文。
3. **PADR**表示PPPoE会话处于发现阶段，并已经发送PADR报文。
4. **UP**表示PPPoE会话建立成功。



总结

- PPPoE帧为什么要降低MTU大小?
- 在配置PPPoE时， dialer bundle命令的作用是什么?



1. 以太网中默认最大支持1500字节的有效载荷。PPPoE头部长度为6字节，PPP协议ID长度为2字节，所以PPPoE帧中的MTU不能超过1492字节。
2. **dialer bundle**命令用来指定Dialer接口使用的Dialer bundle。设备通过Dialer bundle将物理接口与拨号接口关联起来。


谢谢
www.huawei.com


网络地址转换
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

随着Internet的发展和网络应用的增多，IPv4地址枯竭已经成为制约网络发展的瓶颈。尽管IPv6可以从根本上解决IPv4地址空间不足的问题，但目前众多的网络设备和网络应用仍是基于IPv4的，因此在IPv6广泛应用之前，一些过渡技术的使用是解决这个问题的主要技术手段。

网络地址转换技术NAT（Network Address Translation）主要用于实现位于内部网络的主机访问外部网络的功能。当局域网内的主机需要访问外部网络时，通过NAT技术可以将其私网地址转换为公网地址，并且多个私网用户可以共用一个公网地址，这样既可保证网络互通，又节省了公网地址。





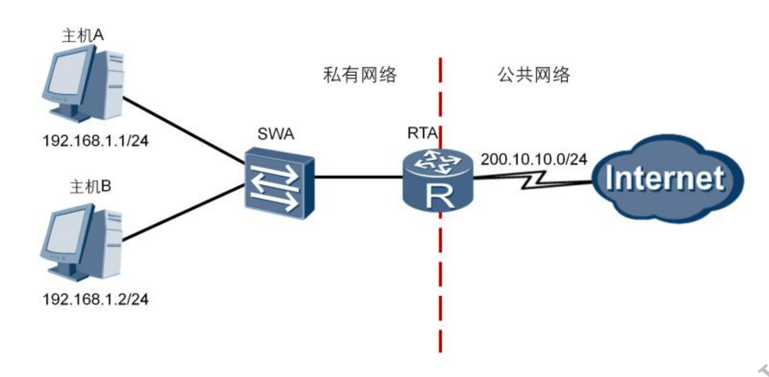
学习目标

学完本课程后，您应该能：

- 掌握NAT的工作原理
- 掌握NAT的基本配置



NAT应用场景



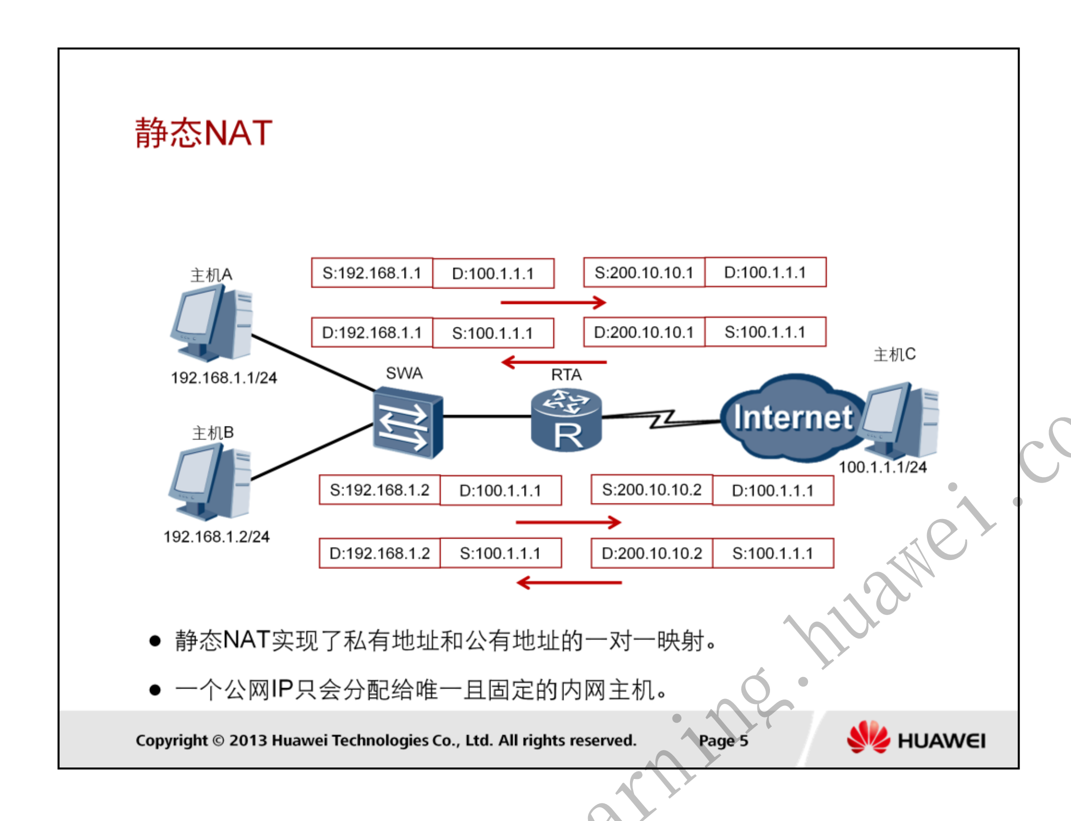
- 企业或家庭所使用的网络为私有网络，使用的是私有地址；运营商维护的网络为公共网络，使用的是公有地址。私有地址不能在公网中路由。
- NAT一般部署在连接内网和外网的网关设备上。

 Page 4



随着网络设备的数量不断增长，对IPv4地址的需求也不断增加，导致可用IPv4地址空间逐渐耗尽。解决IPv4地址枯竭问题的权宜之计是分配可重复使用的各类私网地址段给企业内部或家庭使用。但是，私有地址不能在公网中路由，即私网主机不能与公网通信，也不能通过公网与另外一个私网通信。

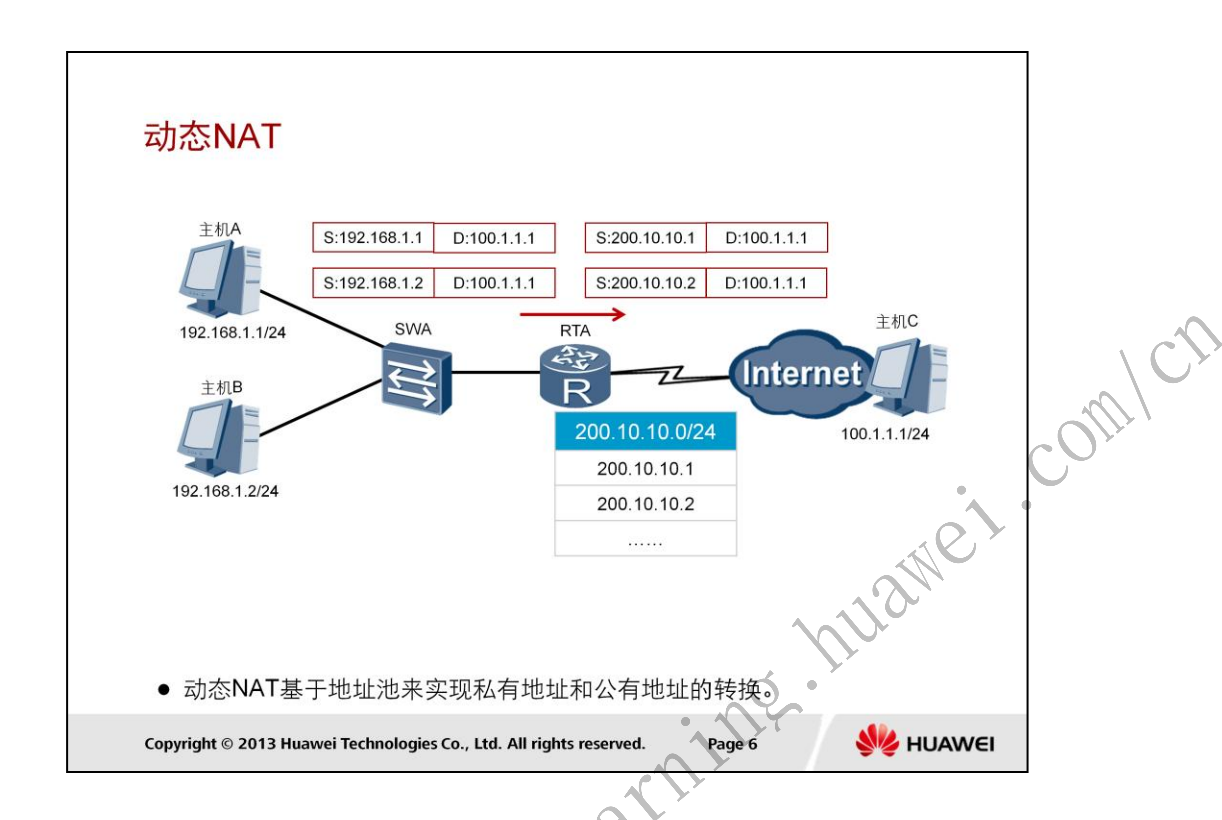
NAT是将IP数据报报头中的IP地址转换为另一个IP地址的过程，主要用于实现内部网络（私有IP地址）访问外部网络（公有IP地址）的功能。NAT一般部署在连接内网和外网的网关设备上。当收到的报文源地址为私网地址、目的地址为公网地址时，NAT可以将源私网地址转换成一个公网地址。这样公网目的地就能够收到报文，并做出响应。此外，网关上还会创建一个NAT映射表，以便判断从公网收到的报文应该发往的私网目的地址。



NAT的实现方式有多种，适用于不同的场景。

静态NAT实现了私有地址和公有地址的一对一映射。如果希望一台主机优先使用某个关联地址，或者想要外部网络使用一个指定的公网地址访问内部服务器时，可以使用静态NAT。但是在大型网络中，这种一对一的IP地址映射无法缓解公用地址短缺的问题。

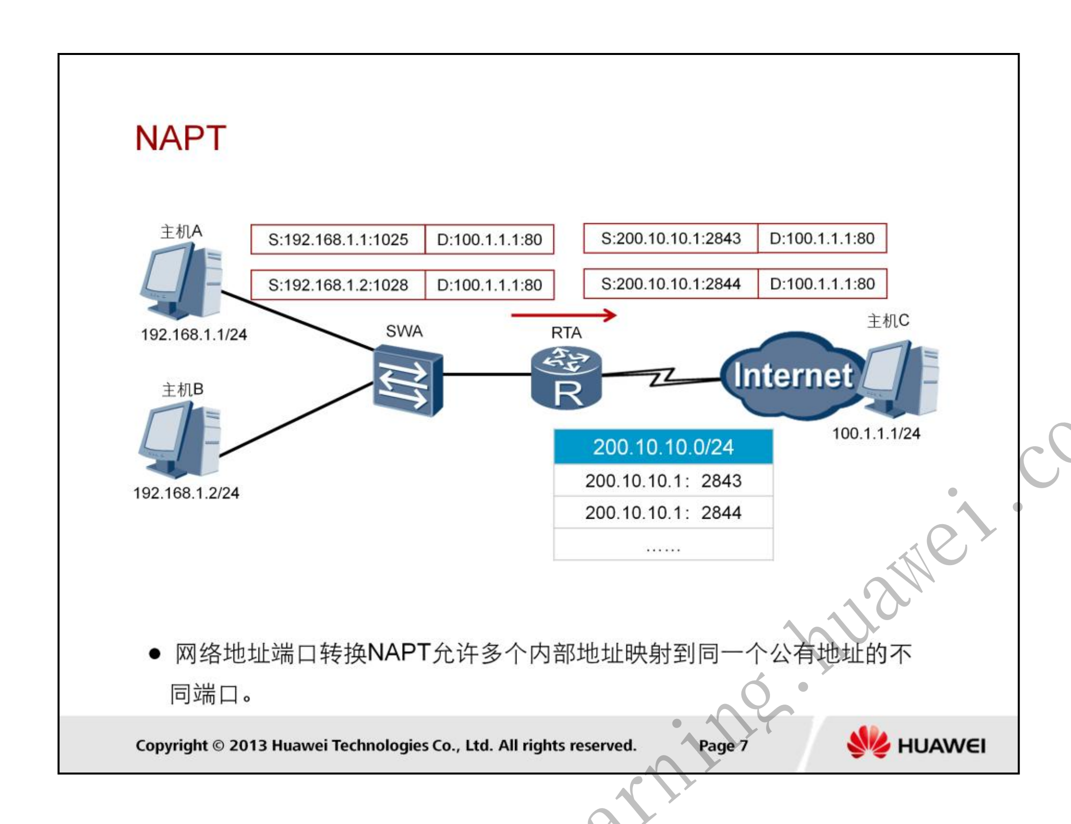
在本示例中，源地址为192.168.1.1的报文需要发往公网地址100.1.1.1。在网关RTA上配置了一个私网地址192.168.1.1到公网地址200.10.10.1的映射。当网关收到主机A发送的数据包后，会先将报文中的源地址192.168.1.1转换为200.10.10.1，然后转发报文到目的设备。目的设备回复的报文目的地址是200.10.10.1。当网关收到回复报文后，也会执行静态地址转换，将200.10.10.1转换成192.168.1.1，然后转发报文到主机A。和主机A在同一个网络中其他主机，如主机B，访问公网的过程也需要网关RTA做静态NAT转换。



动态NAT通过使用地址池来实现。

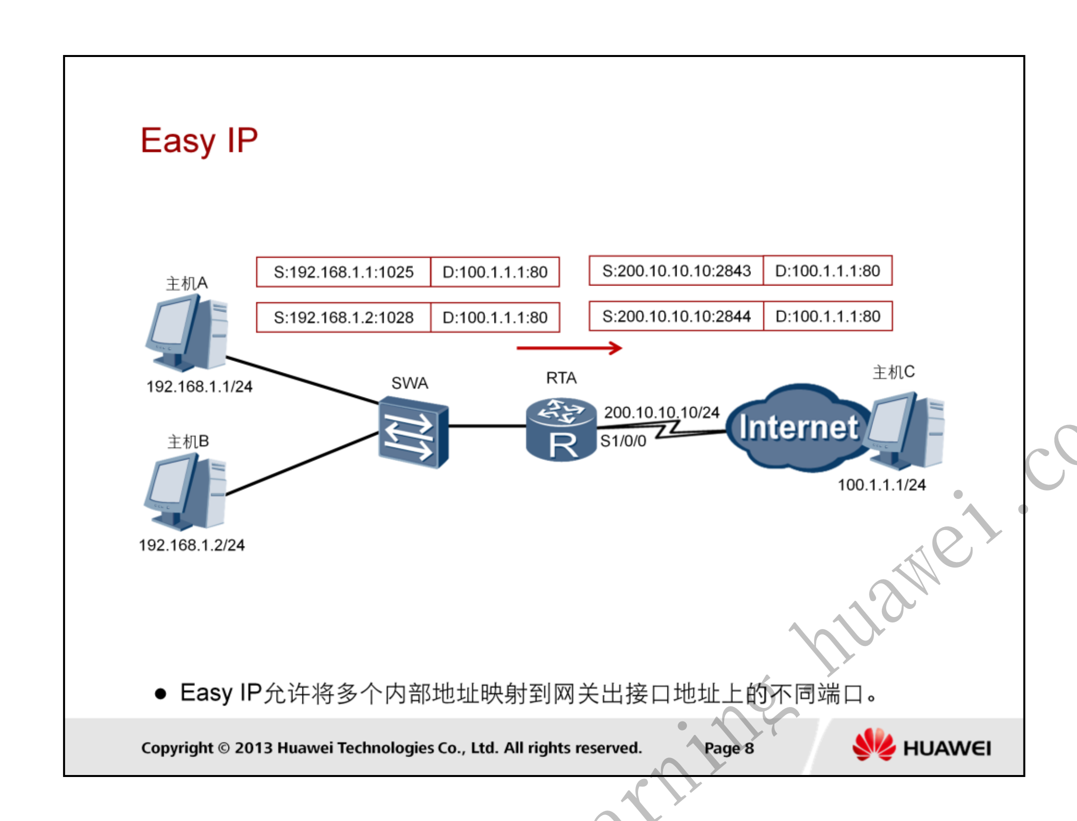
本示例中，当内部主机A和主机B需要与公网中的目的主机通信时，网关RTA会从配置的公网地址池中选择一个未使用的公网地址与之做映射。每台主机都会分配到地址池中的一个唯一地址。当不需要此连接时，对应的地址映射将会被删除，公网地址也会被恢复到地址池中待用。当网关收到回复报文后，会根据之前的映射再次进行转换之后转发给对应主机。

动态NAT地址池中的地址用尽以后，只能等待被占用的公用IP被释放后，其他主机才能使用它来访问公网。



网络地址端口转换NAPT（Network Address Port Translation）允许多个内部地址映射到同一个公有地址的不同端口。

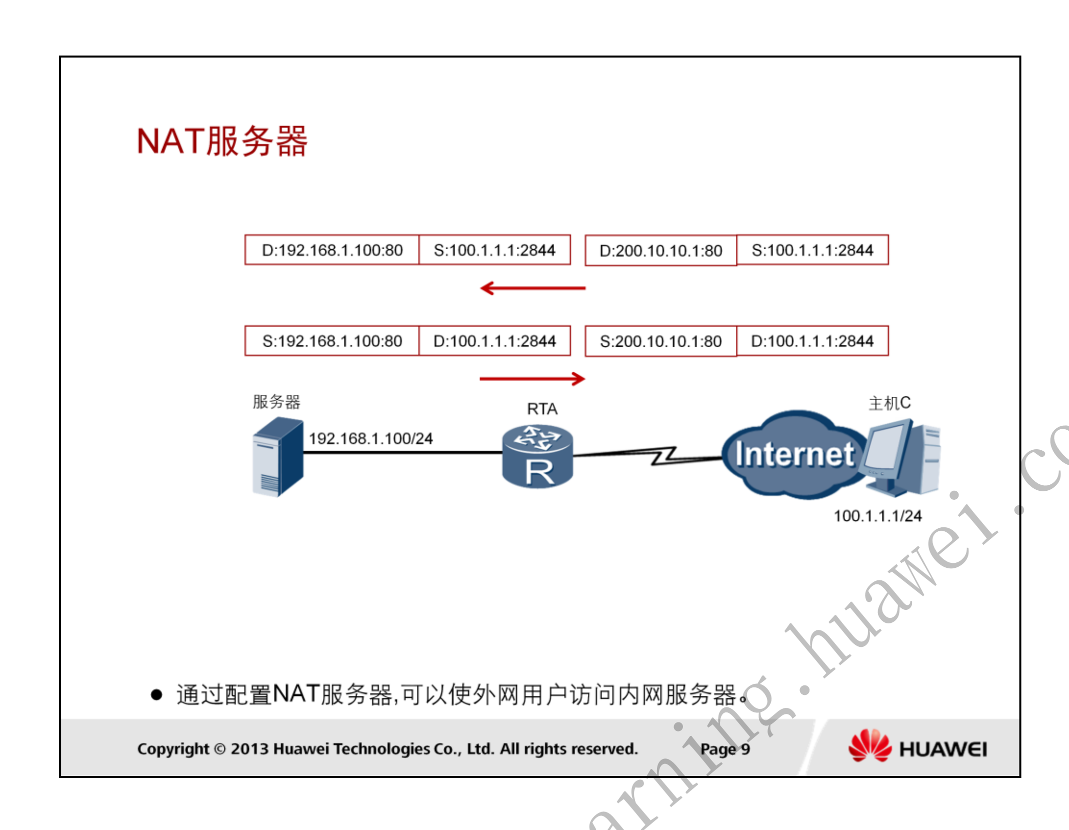
本例中，RTA收到一个私网主机发送的报文，源IP地址是192.168.1.1，源端口号是1025，目的IP地址是100.1.1.1，目的端口是80。RTA会从配置的公网地址池中选择一个空闲的公网IP地址和端口号，并建立相应的NAPT表项。这些NAPT表项指定了报文的私网IP地址和端口号与公网IP地址和端口号的映射关系。之后，RTA将报文的源IP地址和端口号转换成公网地址200.10.10.1和端口号2843，并转发报文到公网。当网关RTA收到回复报文后，会根据之前的映射表再次进行转换之后转发给主机A。主机B同理。



Easy IP适用于小规模局域网中的主机访问Internet的场景。小规模局域网通常部署在小型的网吧或者办公室中，这些地方内部主机不多，出接口可以通过拨号方式获取一个临时公网IP地址。Easy IP可以实现内部主机使用这个临时公网IP地址访问Internet。

本示例说明了Easy IP的实现过程。RTA收到一个主机A访问公网的请求报文，报文的源IP地址是192.168.1.1，源端口号是1025。RTA会建立Easy IP表项，这些表项指定了源IP地址和端口号与出接口的公网IP地址和端口号的映射关系。之后，根据匹配的Easy IP表项，将报文的源IP地址和端口号转换成出接口的IP地址和端口号，并转发报文到公网。报文的源IP地址转换成200.10.10.10/24，相应的端口号是2843。

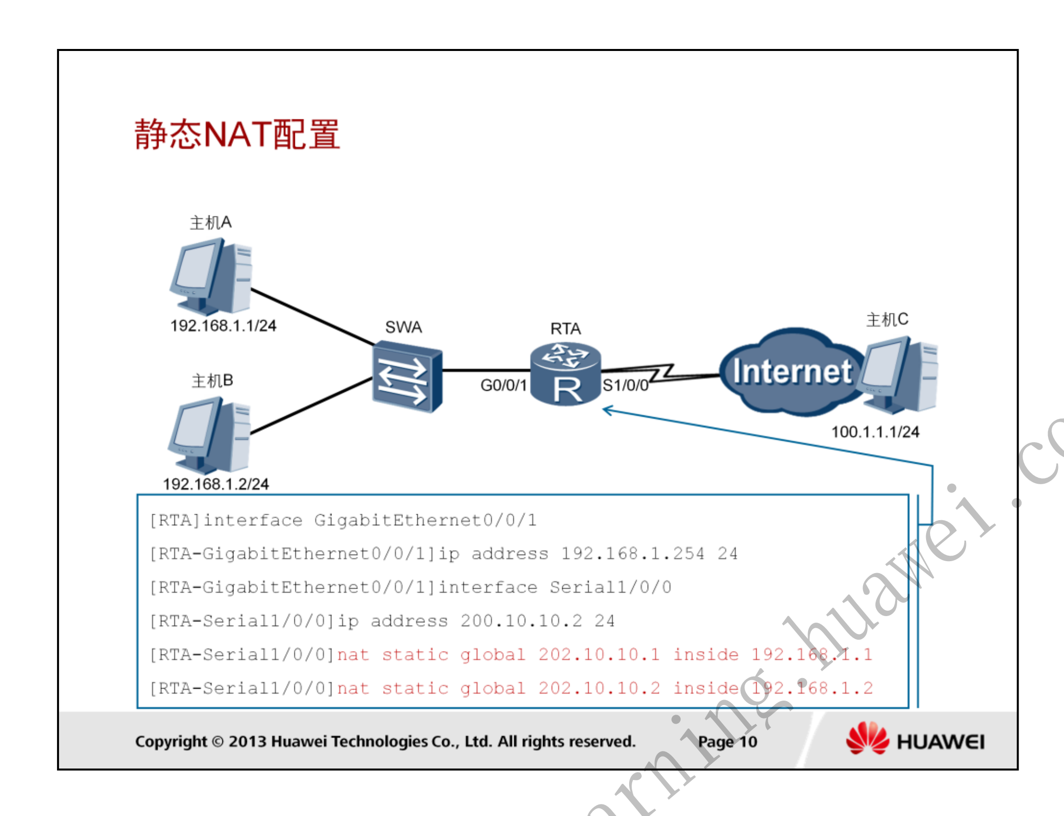
路由器收到回复报文后，会根据报文的目的IP地址和端口号，查询Easy IP表项。路由器根据匹配的Easy IP表项，将报文的目的IP地址和端口号转换成私网主机的IP地址和端口号，并转发报文到主机。



NAT在使内网用户访问公网的同时，也屏蔽了公网用户访问私网主机的需求。当一个私网需要向公网用户提供Web和FTP服务时，私网中的服务器必须随时可供公网用户访问。

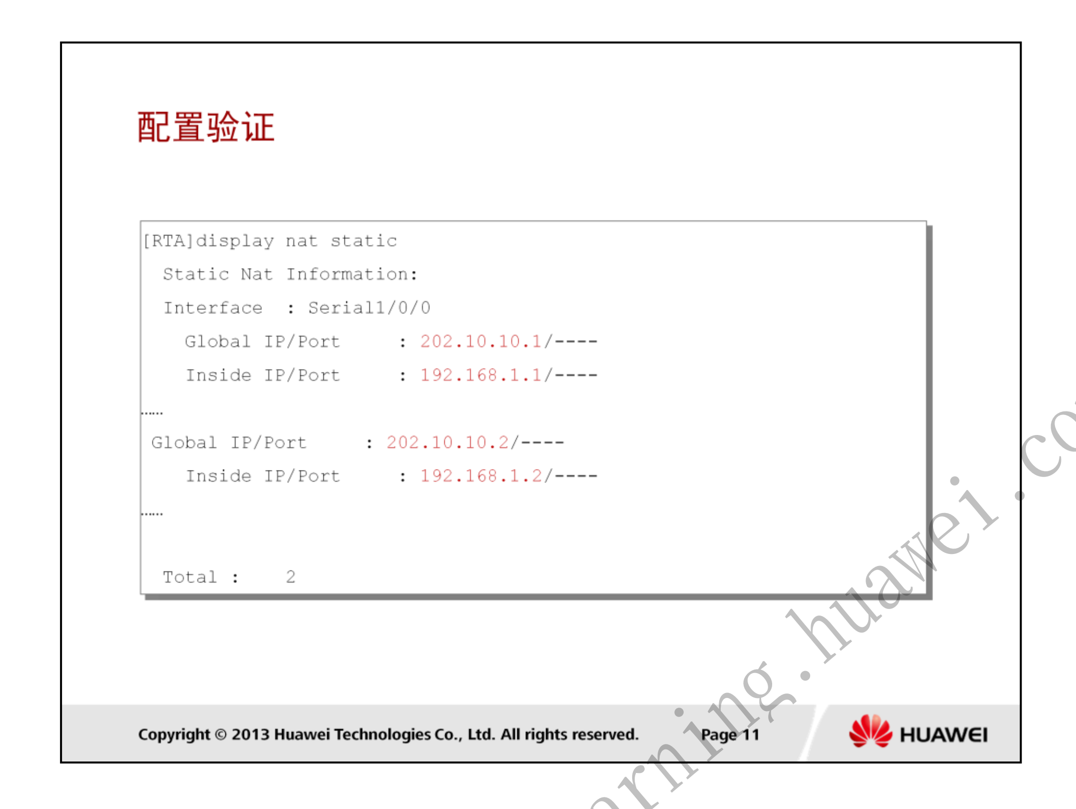
NAT服务器可以实现这个需求，但是需要配置服务器私网IP地址和端口号转换为公网IP地址和端口号并发布出去。路由器在收到一个公网主机的请求报文后，根据报文的目的IP地址和端口号查询地址转换表项。路由器根据匹配的地址转换表项，将报文的目的IP地址和端口号转换成私网IP地址和端口号，并转发报文到私网中的服务器。

本例中，主机C需要访问私网服务器，发送报文的目的IP地址是200.10.10.1，目的端口号是80。RTA收到此报文后会查找地址转换表项，并将目的IP地址转换成192.168.1.1，目的端口号保持不变。服务器收到报文后会进行响应，RTA收到私网服务器发来的响应报文后，根据报文的源IP地址192.168.1.1和端口号80查询地址转换表项。然后，路由器根据匹配的地址转换表项，将报文的源IP地址和端口号转换成公网IP地址200.10.10.1和端口号80，并转发报文到目的公网主机。



nat static global { *global-address*} **inside** {*host-address* } 命令用于创建静态NAT。

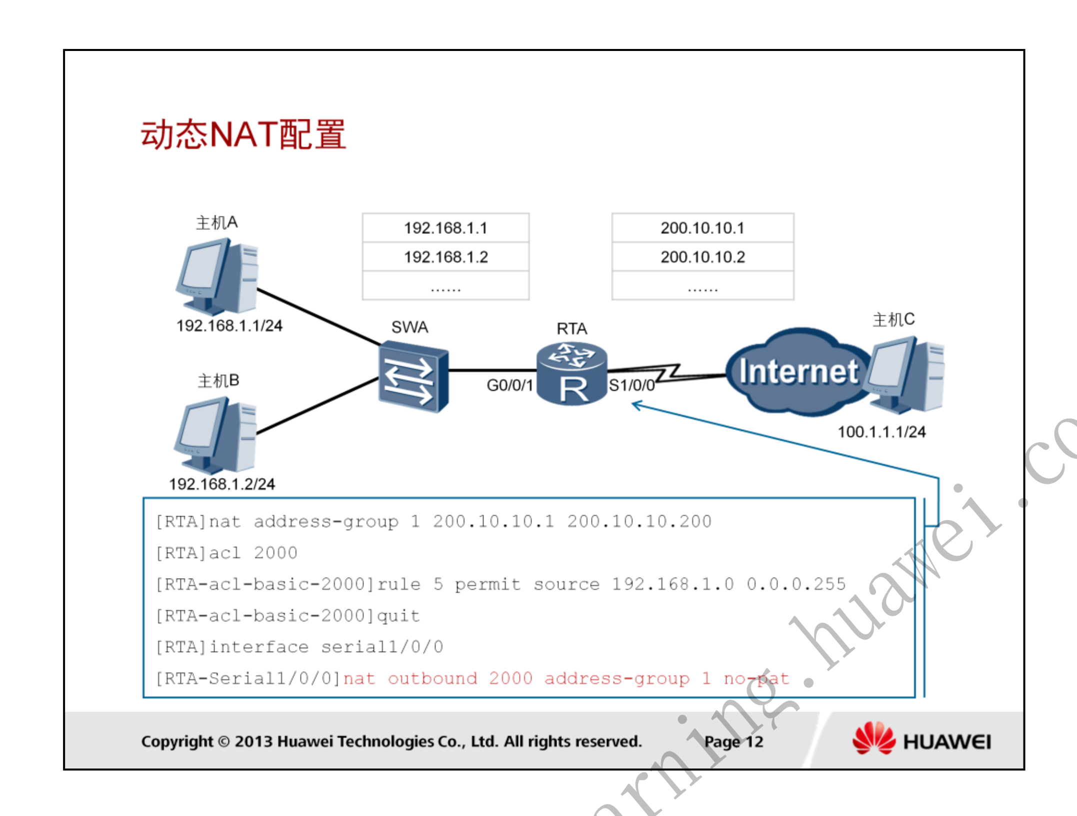
1. global参数用于配置外部公网地址。
2. inside参数用于配置内部私有地址。



命令**display nat static**用于查看静态NAT的配置。

Global IP/Port表示公网地址和服务端口号。

Inside IP/Port表示私有地址和服务端口号。



nat outbound命令用来将一个访问控制列表ACL和一个地址池关联起来，表示ACL中规定的地址可以使用地址池进行地址转换。ACL用于指定一个规则，用来过滤特定流量。后续将会介绍有关ACL的详细信息。

nat address-group命令用来配置NAT地址池。

本示例中使用 **nat outbound** 命令将ACL 2000与待转换的192.168.1.0/24网段的流量关联起来，并使用地址池1（**address-group 1**）中的地址进行地址转换。**no-pat**表示只转换数据报文的地址而不转换端口信息。

配置验证

```
[RTA]display nat address-group 1
 NAT Address-Group Information:
 --------------------------------------
 Index    Start-address        End-address
 1        200.10.10.1          200.10.10.200

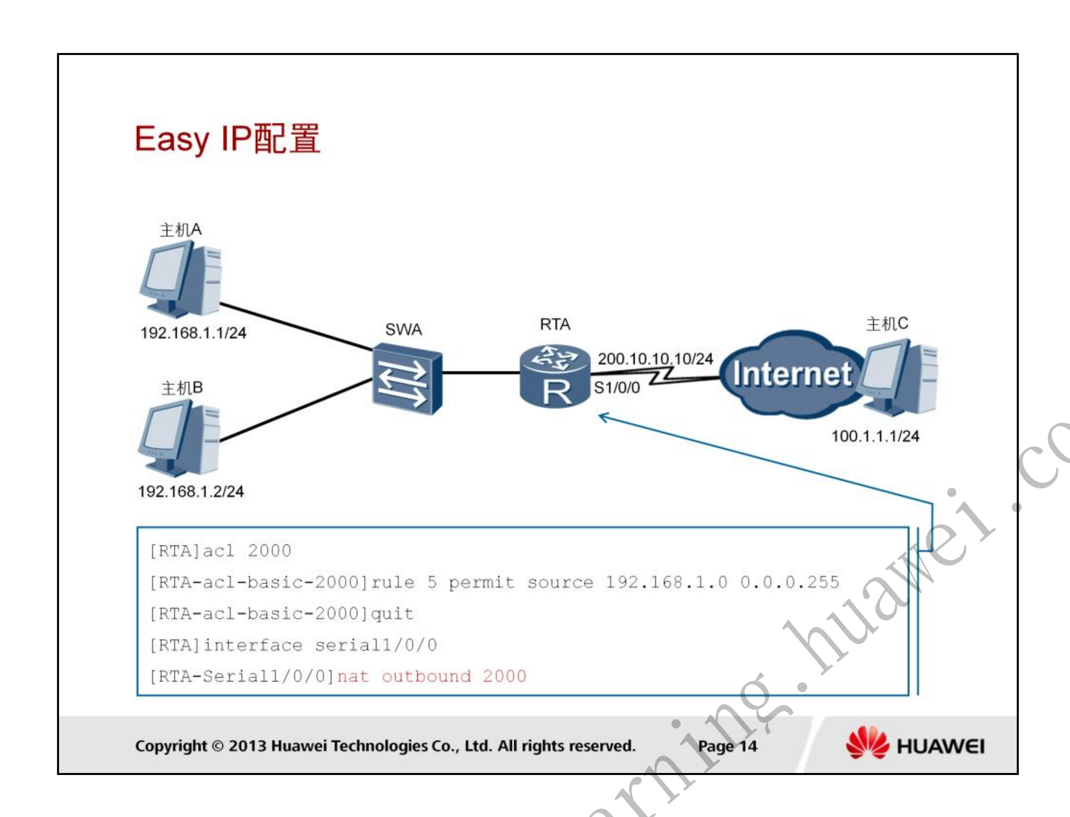
[RTA]display nat outbound
 NAT Outbound Information:
 -----------------------------------------------------------------
 Interface            Acl      Address-group/IP/Interface       Type
 -----------------------------------------------------------------
 Serial1/0/0        2000                            1          no-pat
 -----------------------------------------------------------------
  Total : 1
```

 Page 13 HUAWEI

display nat address-group *group-index*命令用来查看NAT地址池配置信息。

命令**display nat outbound**用来查看动态NAT配置信息。

可以用这两条命令验证动态NAT的详细配置。在本示例中，指定接口Serial 1/0/0与ACL关联在一起，并定义了用于地址转换的地址池1。参数**no-pat**说明没有进行端口地址转换。



nat outbound *acl-number*命令用来配置Easy-IP地址转换。Easy IP的配置与动态NAT的配置类似，需要定义ACL和**nat outbound**命令，主要区别是Easy IP不需要配置地址池，所以**nat outbound**命令中不需要配置参数**address-group**。

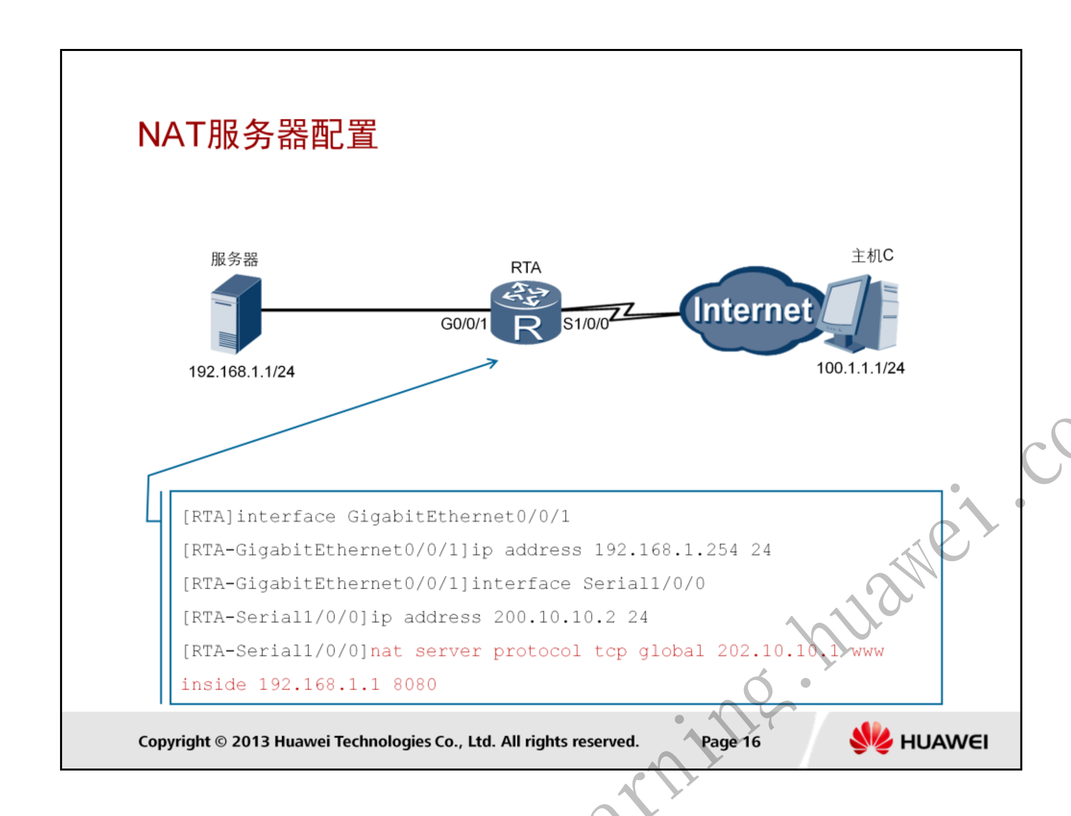
在本示例中，命令**nat outbound 2000**表示对ACL 2000定义的地址段进行地址转换，并且直接使用Serial1/0/0接口的IP地址作为NAT转换后的地址。

配置验证

```
[RTA]display nat outbound
 NAT Outbound Information:
 ---------------------------------------------------------------------
 Interface         Acl      Address-group/IP/Interface       Type
 ---------------------------------------------------------------------
 Serial1/0/0       2000       200.10.10.1                   easyip
 ---------------------------------------------------------------------
  Total : 1
```


命令**display nat outbound**用于查看命令**nat outbound**的配置结果。

Address-group/IP/Interface表项表明接口和ACL已经关联成功，type表项表明Easy IP已经配置成功。



nat server [**protocol** {*protocol-number* | icmp | tcp | udp} **global** { *global-address* | current-interface *global-port*} **inside** {*host-address* *host-port* } **vpn-instance** *vpn-instance-name* **acl** *acl-number* **description** *description*]命令用来定义一个内部服务器的映射表，外部用户可以通过公网地址和端口来访问内部服务器。

参数protocol指定一个需要地址转换的协议；

参数*global-address*指定需要转换的公网地址；

参数inside指定内网服务器的地址。

配置验证

```
[RTA]display nat server
 Nat Server Information:
 Interface  : Serial1/0/0
   Global IP/Port     : 202.10.10.1/80(www)
   Inside IP/Port     : 192.168.1.1/8080
   Protocol : 6(tcp)
   VPN instance-name  : ----
   Acl number         : ----
   Description : ----

 Total :    1
```

 Page 17



display nat server命令用于查看详细的NAT服务器配置结果。

可以通过此命令验证地址转换的接口、全局和内部IP地址以及关联的端口号。在本示例中，全局地址202.10.10.1和关联的端口号80（www）分别被转换成内部服务器地址192.168.1.1和端口号8080。



总结

- 哪种NAT转换允许服务器既能被内部访问又能被外部访问?
- NAPT有什么功能和特点?



1. 通过NAT内部服务器配置，将公网地址与一个私网服务器地址绑定，在地址转换后，外网主机便可以通过公有地址访问内网服务器。同时，内部用户可以通过服务器的私网地址访问内网服务器。
2. NAPT是基于端口的转换，而不是基于IP地址的转换。NAPT允许多个内部地址映射到同一个公有地址的不同端口。


谢谢
www.huawei.com


企业无线解决方案
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

一般地，企业网络与Internet的连接都是有线连接；为了增强企业网络与Internet连接的可靠性，我们还可以通过WWAN增加企业网络与Internet的无线连接。这样，当发生不可预见的故障而导致企业网络与Internet的有线连接中断时，无线连接就可以接管故障，保证企业网络与Internet的连通性，进而保障企业网络业务的连续性和可用性。

HUAWEI

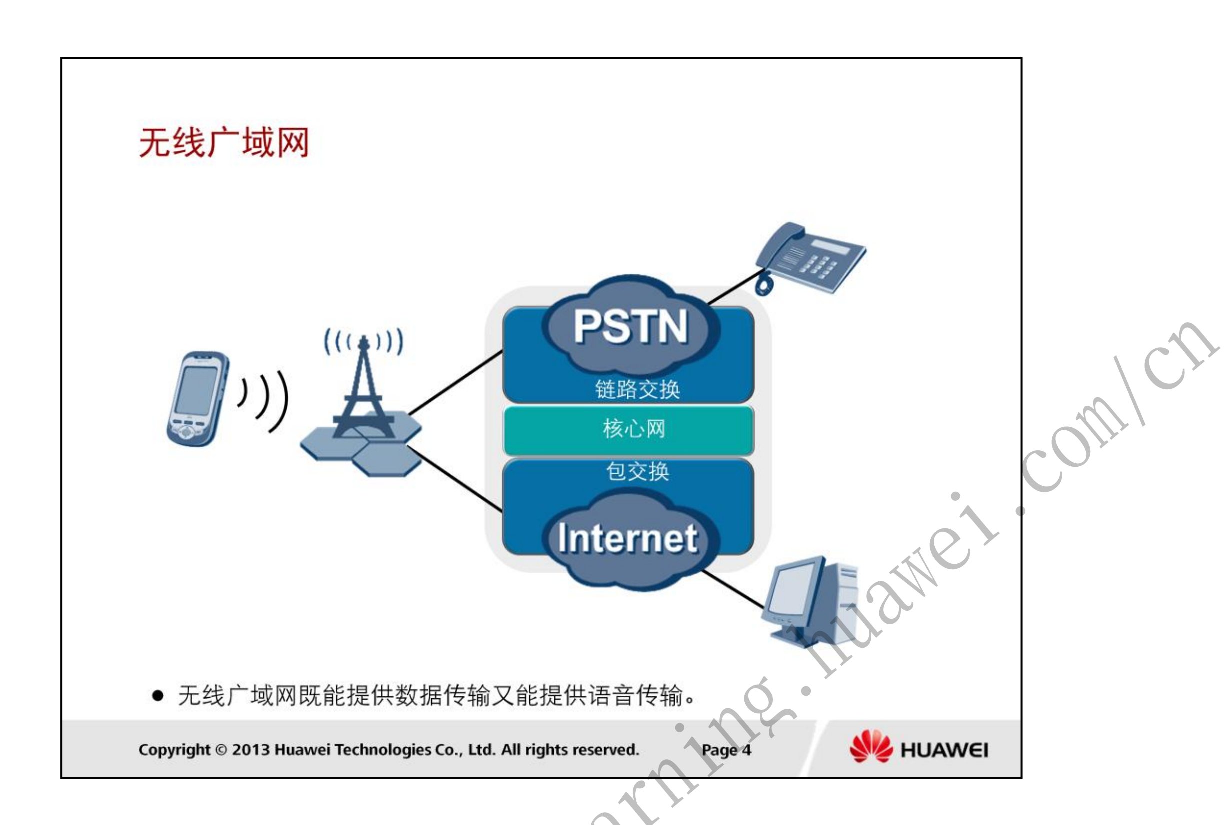




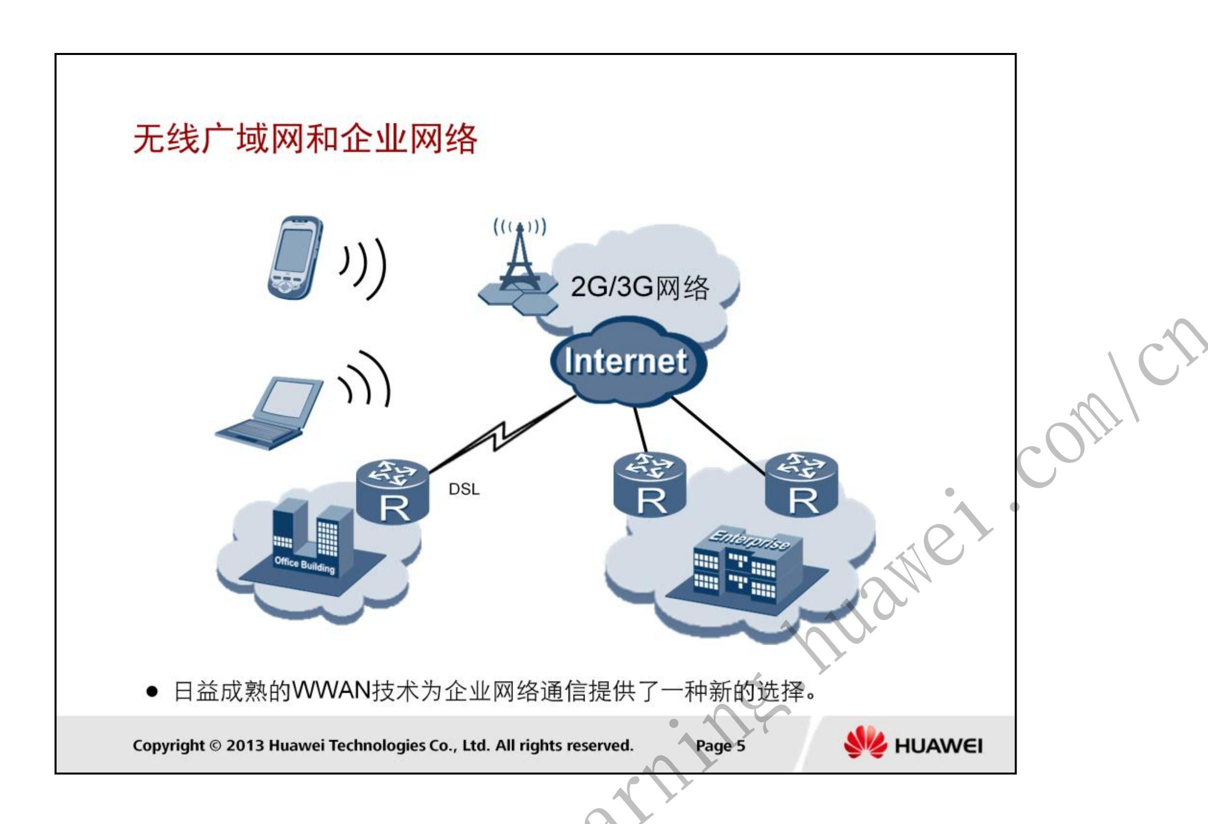
学习目标

学完本课程后，您应该能：

- 解释2G和3G网络是如何作为企业网络的备份的
- 解释cellular接口进行故障切换的过程

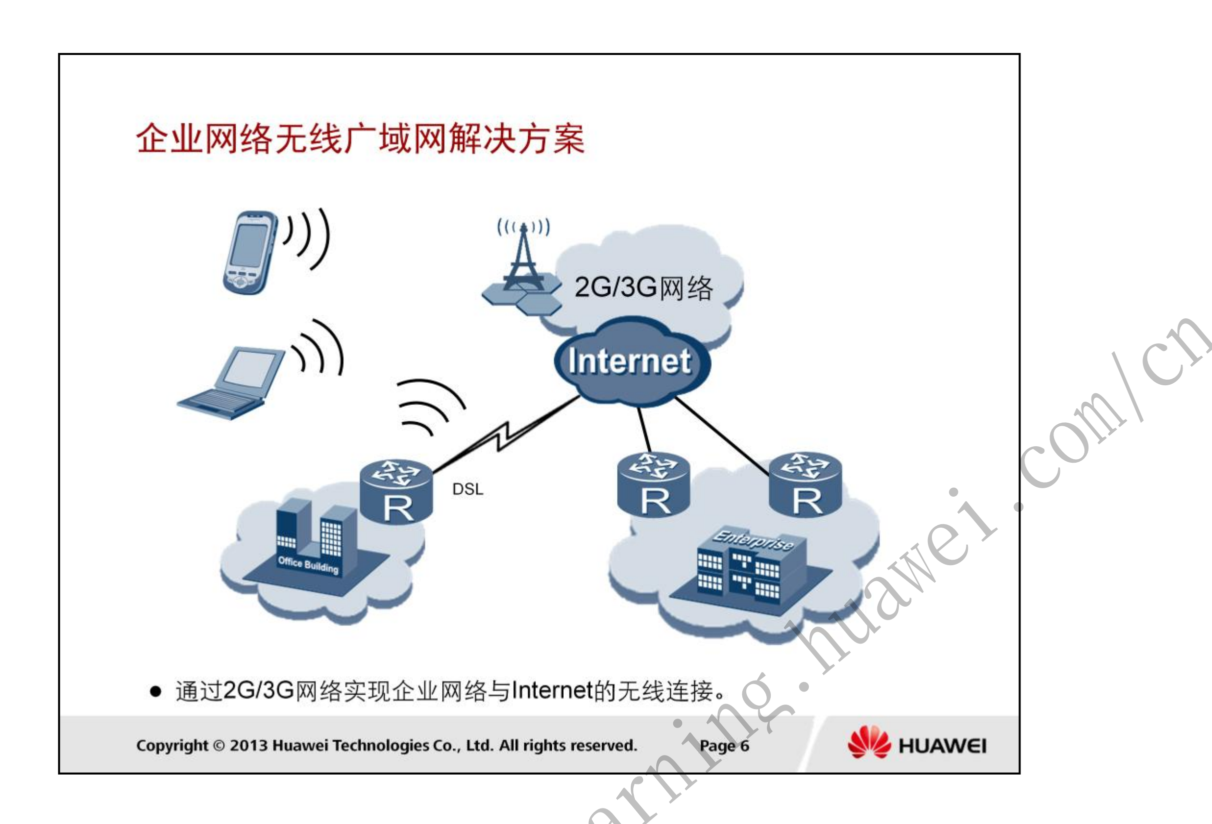


无线广域网WWAN（Wireless Wide Area Network）目前已经成为了全球通信系统的核心组成部分，我们所熟悉的2G网络、3G网络和4G网络（LTE）等等都是WWAN的典型代表。通过WWAN，用户几乎可以在任何时间和任何地点利用移动终端设备进行语音和数据通信。



WWAN的存在，使得旅行途中的企业员工或地处偏远地区的企业员工可以随时通过移动终端访问Internet，进而能够访问与Internet相连的企业网络。在此情形下，最需要关注的是WWAN的传输速率和可用服务。

WWAN的发展大致经历了从1G，2G（如GSM），2.5G（如GPRS），2.75G（EDGE），3G（如WCDMA，HSPA，HSPA+）到4G（如LTE）的过程。随着技术的进步，WWAN能够支持的传输速率也在不断提高。例如，HSPA支持的最大下行链路容量可以达到14 Mbit/s，HSPA+支持的最大下行链路容量可以达到168 Mbit/s。目前，LTE技术已经开始投入实际应用，它可以支持更高速率的数据传输业务。



前面提到，旅行途中的企业员工或地处偏远地区的企业员工可以利用WWAN随时通过移动终端访问Internet，进而能够访问与Internet相连的企业网络。一般地，企业网络与Internet的连接都是有线连接；为了增强企业网络与Internet连接的可靠性，我们还可以通过WWAN增加企业网络与Internet的无线连接。这样，当发生不可预见的故障而导致企业网络与Internet的有线连接中断时，无线连接就可以保证企业网络与Internet的连通性。

例如，本例中的DSL连接中断时，路由器与基站之间的无线连接可接管故障，从而保证企业网络与Internet的连通性，进而保障企业网络业务的连续性和可用性。



华为AR2200路由器使用了3G-HSPA+7接口卡来提供2G和3G网络接口，该接口也称为蜂窝接口（cellular interface）。3G-HSPA+7接口卡有两个3G天线接口，用来发送和接收3G业务数据，其中一个接口是主接口，另一个是副接口，都支持2G的GSM/GPRS/EDGE、和3G的WCDMA/HSPA/HSPA+标准。鞭状天线直接安装在AR路由器上；当路由器安装在桌子上或壁挂时，推荐使用鞭状天线。远程天线包含一条3米长的馈线；当路由器安装在机柜里或机架上时，推荐使用远程天线。

建立3G网络连接




```
<Huawei>system-view
[Huawei]interface cellular 0/0/0
[Huawei-cellular0/0/0]ip address ppp-negotiate
[Huawei-cellular0/0/0]profile create 1 static 3GNET
[Huawei-cellular0/0/0]mode wcdma wcdma-precedence
[Huawei-cellular0/0/0]quit
```

- 在cellular接口上定义3G网络参数。

ARG3系列路由器的3G蜂窝接口传输射频信号，并支持PPP链路层协议和IP网络层协议。

interface cellular命令用来进入3G cellular接口视图。

ip address ppp-negotiate命令用来配置蜂窝接口通过PPP协商获取IP地址。

profile create *profile-number* { **dynamic** | **static** *apn* }命令用来创建3G modem的参数描述模板并配置接入点名称APN（Access Point Name）。*profile-number*参数用来指定模板的标识符，**static**或**dynamic**选项用来配置静态配置或动态分配APN。APN用来标识WCDMA网络的业务种类。

mode wcdma { **gsm-only** | **gsm-precedence** | **wcdma-only** | **wcdma-precedence** }命令用来配置3G modem连接WCDMA网络的方式。如果3G调制解调器安装了通用用户识别模块USIM（Universal Subscriber Identity Module），可以执行**mode wcdma**命令来配置3G调制解调器的WCDMA网络连接模式。如果指定了**wcma-precedence**参数，则会优先使用WCDMA模式。

设置拨号控制中心




```
[Huawei]dialer-rule
[Huawei-dialer-rule]dialer-rule 1 ip permit
[Huawei-dialer-rule]quit
[Huawei]interface cellular 0/0/0
[Huawei-cellular0/0/0]dialer enable-circular
[Huawei-cellular0/0/0]dialer-group 1
[Huawei-cellular0/0/0]dialer number *99#
```

 Page 9



拨号控制中心DCC（Dial Control Center）允许链路激活蜂窝连接。

dialer-rule命令用来进入Dialer-rule视图。

dialer-rule *dialer-rule-number* { **acl** { *acl-number* | **name** *acl-name* } | **ip** { **deny** | **permit** } | **ipv6** { **deny** | **permit** } }命令用来配置某个拨号访问组对应的拨号访问控制列表，指定引发DCC呼叫的条件。*dialer-rule-number* 代表拨号访问组（dialer access group）的编号。

dialer enable-circular命令用来使能轮询DCC（Circular DCC）功能。ARG3系列路由器支持两种DCC模式：轮询DCC（Circular DCC）和共享DCC（Resource-Shared DCC）方式。两种DCC模式分别应用于不同的场景。轮询DCC适用于物理链路较多，连接情况复杂的大中型站点；共享DCC适用于可用物理链路较少，但连接需求较多的中小型站点。

dialer-group命令用来将接口置于一个拨号访问组，要想使DCC正常发送报文，必须配置正确的DCC拨号控制列表，并将对应接口（如物理接口、Dialer接口）通过**dialer-group**命令关联到拨号控制列表。

dialer number *dial-number* [**autodial**]命令用来配置呼叫一个对端的拨号号码。

配置NAT角色和静态路由




```
[Huawei]acl number 3002
[Huawei-acl-adv-3002]rule 5 permit ip source 192.168.1.0 0.0.0.255
[Huawei-acl-adv-3002]quit
[Huawei]interface cellular 0/0/0
[Huawei-cellular0/0/0]nat outbound 3002
[Huawei-cellular0/0/0]quit

[Huawei]ip route-static 0.0.0.0 0 cellular 0/0/0
```

 Page 10 

如果内网用户使用私网IP地址，则需要配置网络地址转换NAT（Network Address Translation），把私网IP地址转换成蜂窝接口的公网IP地址。因为只存在一个蜂窝接口地址，所以一般使用Easy IP，允许内网用户通过端口地址转换使用唯一的公网IP地址。同时，ACL能够定义可以转换成公网地址的私网地址范围。

nat outbound *acl-number*命令用来配置Easy-IP地址转换。

本示例中，企业内网用户使用了网段192.168.1.0/24，订阅了WCDMA服务，路由器通过DCC功能把企业网络连接到Internet，企业从运营商处获取到APN 3GNET和拨号串*99#。

配置验证

```
<Huawei> display interface Cellular 0/0/0
Cellular0/0/0 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, Cellular0/0/0 Interface
Route Port, The Maximum Transmit Unit is 1500
Internet Address is negotiated, 203.161.70.97/32
Link layer protocol is PPP
LCP opened, IPCP opened
Last physical up time : 2013-06-08 10:53:15
Last physical down time : 2013-06-08 10:53:13
Current system time: 2013-06-08 11:35:23
Modem State: Present
……
```

 Page 11



使用C-DCC和PPP协商建立3G网络并连接成功后，蜂窝接口会被分配一个IP地址。

display interface cellular命令可以用来验证建立的连接，查看接口状态和协商的地址。如果接口没有被分配IP地址，可能是因为没有通信数据在链路上传输，或者是因为链路协商失败，此时系统会提示"**Internet protocol processing : disabled**"（网络协议进程：未使能）。**Modem State**字段表明3G蜂窝接口是否连接到3G调制解调器。

配置验证

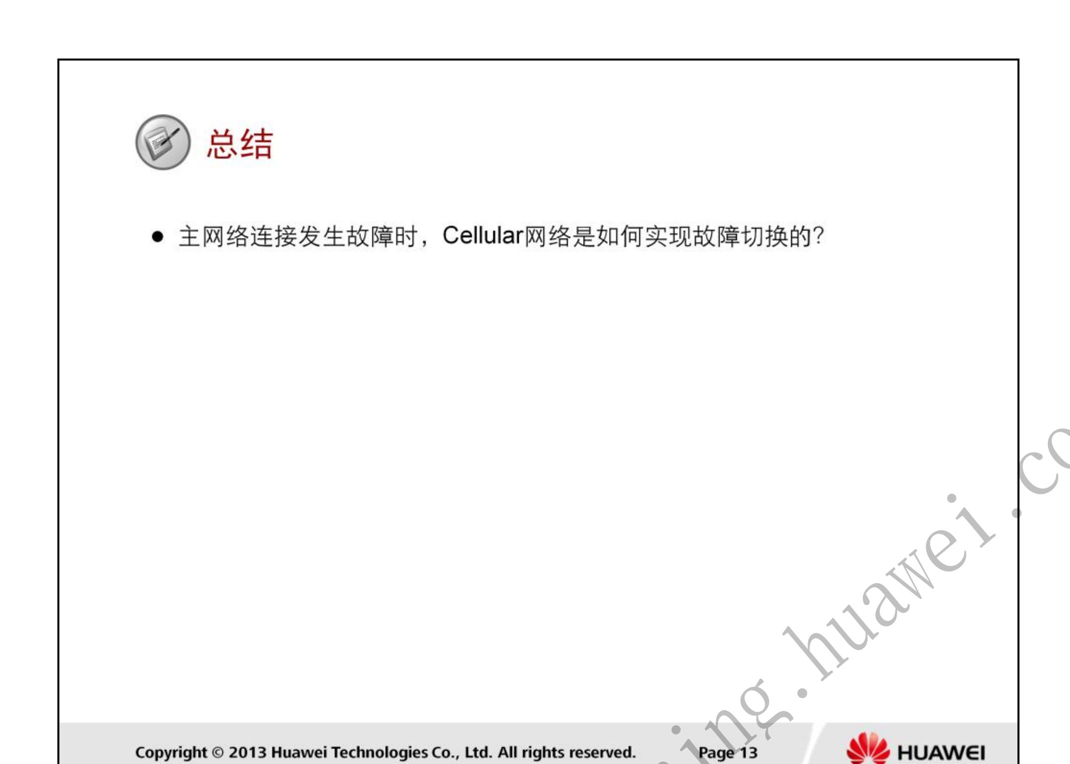
```
[Huawei] display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------
 Interface          Acl      Address-group/IP/Interface       Type
 ----------------------------------------------------------------------
 Cellular0/0/0     3002          203.161.70.97               easyip
 ----------------------------------------------------------------------
  Total : 1
```

- Cellular0/0/0接口上部署了Easy IP。
- 内部地址映射到了Cellular0/0/0接口的IP地址。

 Page 12 

可以再次执行**display nat outbound**命令，验证Easy IP的配置，查看蜂窝备份链路建立情况。从命令回显信息可以看到，蜂窝接口使用Easy IP功能进行地址转换。

本示例中，使用了ACL 3002，网段192.168.1.0/24上的IP地址都可以转换成蜂窝接口的公网IP地址203.161.70.97。



1. 如果主网络连接发生故障，默认静态路由会通过蜂窝接口提供一条备选的无线路由。DCC拨号控制中心会通过PPP协商发起蜂窝连接。


谢谢
www.huawei.com

Module-3

增强企业网络的安全性


访问控制列表
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

企业网络中的设备进行通信时，需要保障数据传输的安全可靠和网络的性能稳定。

访问控制列表ACL（Access Control List）可以定义一系列不同的规则，设备根据这些规则对数据包进行分类，并针对不同类型的报文进行不同的处理，从而可以实现对网络访问行为的控制、限制网络流量、提高网络性能、防止网络攻击等等。

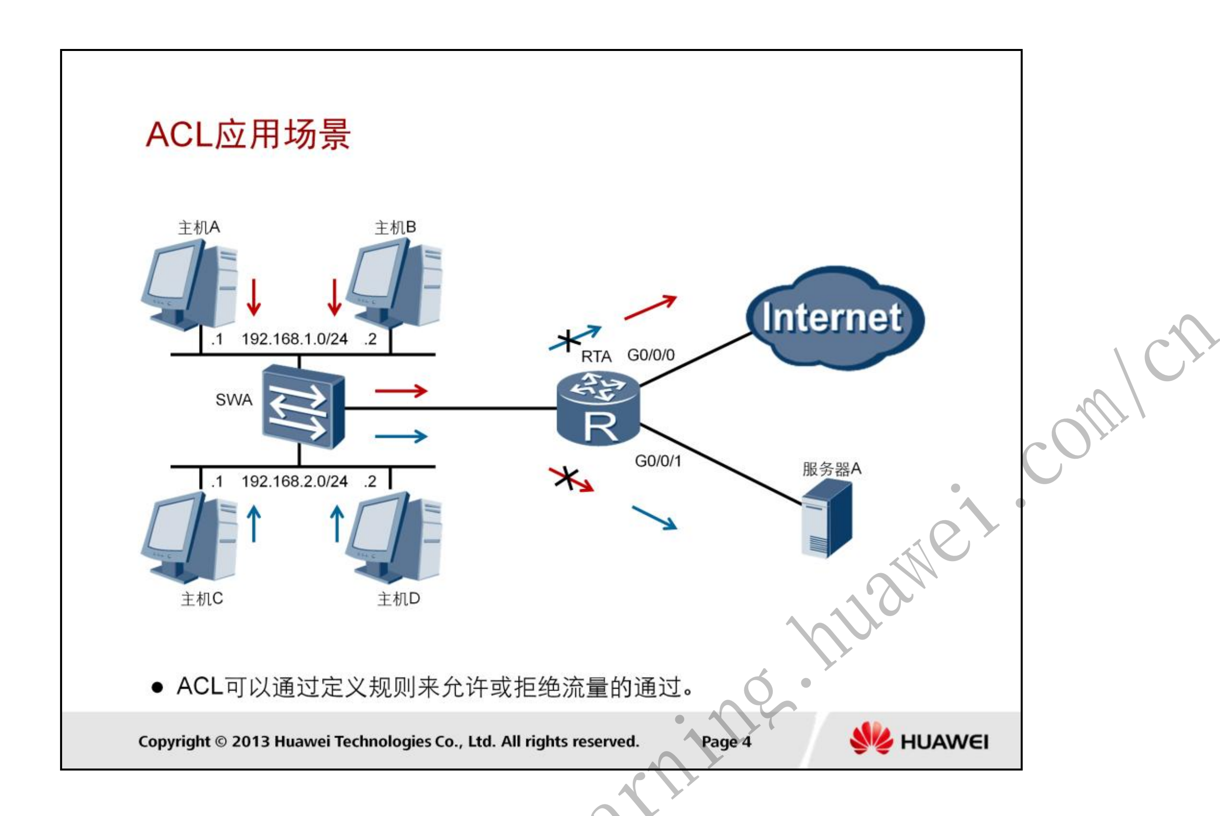




学习目标

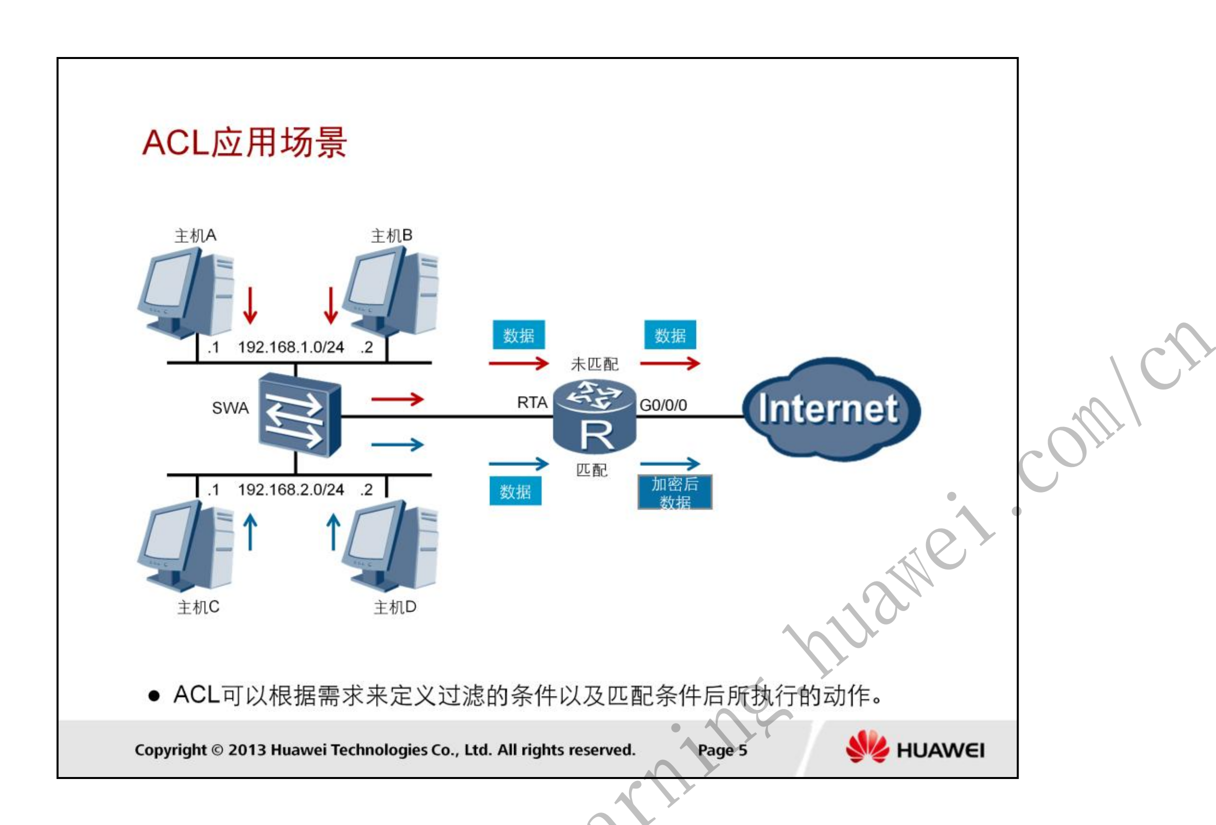
学完本课程后，您应该能：

- 掌握ACL在企业网络中的应用
- 掌握ACL的工作原理
- 掌握ACL的配置



ACL是由一系列规则组成的集合。设备可以通过这些规则对数据包进行分类，并对不同类型的报文进行不同的处理。

本示例中，网关RTA允许192.168.1.0/24中的主机可以访问外网，也就是Internet；而192.168.2.0/24中的主机则被禁止访问Internet。对于服务器A而言，情况则相反。网关允许192.168.2.0/24中的主机访问服务器A，但却禁止192.168.1.0/24中的主机访问服务器A。



设备可以依据ACL中定义的条件（例如源IP地址）来匹配入方向的数据，并对匹配了条件的数据执行相应的动作。在本示例所述场景中，RTA依据所定义的ACL而匹配到的感兴趣流量来自192.168.2.0/24网络，RTA会对这些感兴趣流量进行加密（虚拟局域网VPN中会进行介绍）之后再转发。

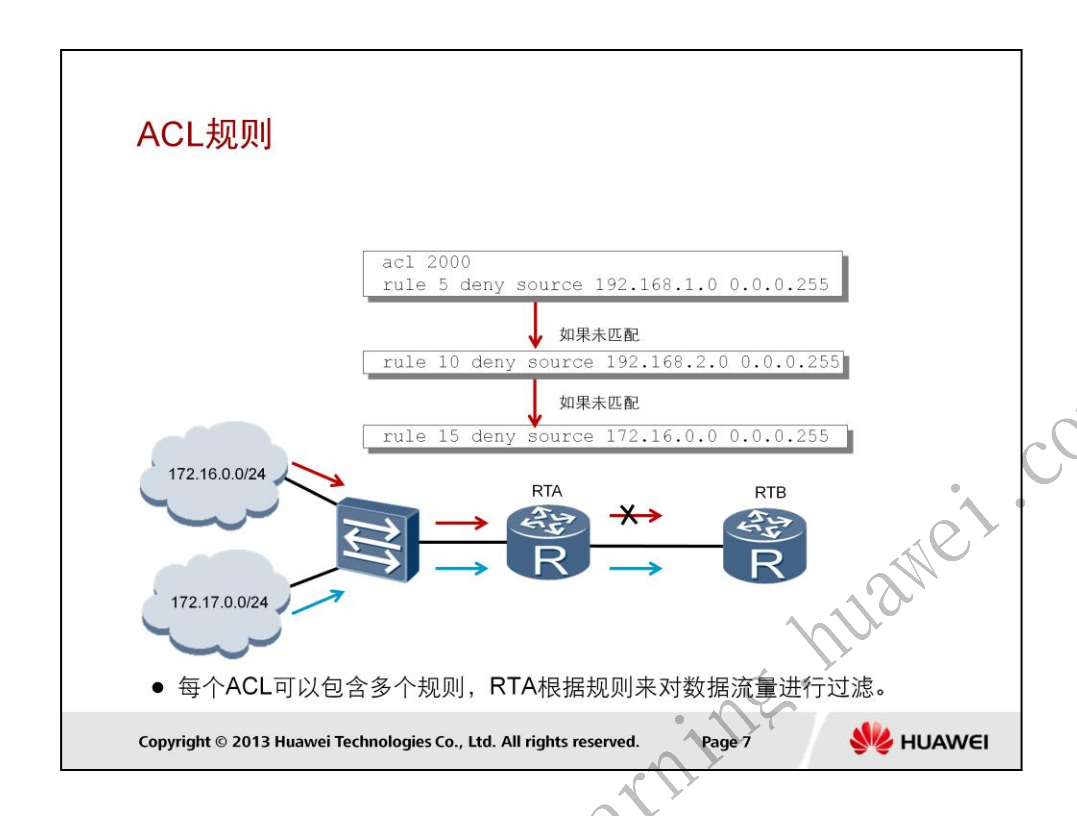
ACL分类

分类	编号范围	参数
基本ACL	2000-2999	源IP地址等
高级ACL	3000-3999	源IP地址、目的IP地址、 源端口、目的端口等
二层ACL	4000-4999	源MAC地址、目的MAC地址、以太帧协议类型等



根据不同的划分规则，ACL可以有不同的分类。最常见的三种分类是基本ACL、高级ACL和二层ACL。

1. 基本ACL可以使用报文的源IP地址、分片标记和时间段信息来匹配报文，其编号取值范围是2000-2999。
2. 高级ACL可以使用报文的源/目的IP地址、源/目的端口号以及协议类型等信息来匹配报文。高级ACL可以定义比基本ACL更准确、更丰富、更灵活的规则，其编号取值范围是3000-3999。
3. 二层ACL可以使用源/目的MAC地址以及二层协议类型等二层信息来匹配报文，其编号取值范围是4000-4999。

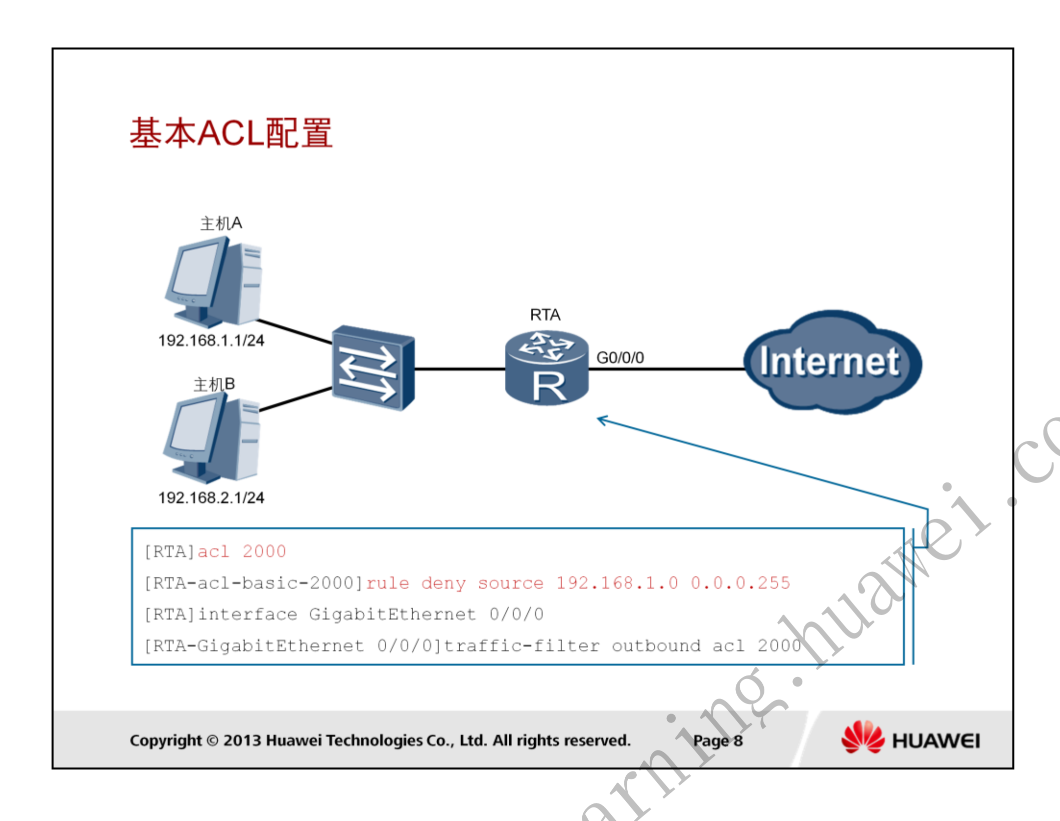


一个ACL可以由多条“**deny | permit**”语句组成，每一条语句描述了一条规则。设备收到数据流量后，会逐条匹配ACL规则，看其是否匹配。如果不匹配，则匹配下一条。一旦找到一条匹配的规则，则执行规则中定义的动作，并不再继续与后续规则进行匹配。如果找不到匹配的规则，则设备不对报文进行任何处理。需要注意的是，ACL中定义的这些规则可能存在重复或矛盾的地方。规则的匹配顺序决定了规则的优先级，ACL通过设置规则的优先级来处理规则之间重复或矛盾的情形。

ARG3系列路由器支持两种匹配顺序：配置顺序和自动排序。

1. 配置顺序按ACL规则编号（rule-id）从小到大的顺序进行匹配。设备会在创建ACL的过程中自动为每一条规则分配一个编号，规则编号决定了规则被匹配的顺序。例如，如果将步长设定为5，则规则编号将按照5、10、15…这样的规律自动分配。如果步长设定为2，则规则编号将按照2、4、6、8…这样的规律自动分配。通过设置步长，使规则之间留有一定的空间，用户可以在已存在的两个规则之间插入新的规则。路由器匹配规则时默认采用配置顺序。另外，ARG3系列路由器默认规则编号的步长是5。
2. 自动排序使用“深度优先”的原则进行匹配，即根据规则的精确度排序。

本示例中，RTA收到了来自两个网络的报文。默认情况下，RTA会依据ACL的配置顺序来匹配这些报文。网络172.16.0.0/24发送的数据流量将被RTA上配置的ACL2000的规则15匹配，因此会被拒绝。而来自网络172.17.0.0/24的报文不能匹配访问控制列表中的任何规则，因此RTA对报文不做任何处理，而是正常转发。



acl [**number**] 命令用来创建一个ACL，并进入ACL视图。

rule [*rule-id*] { **deny** | **permit** } **source** { *source-address source-wildcard* | **any** } 命令用来增加或修改ACL的规则。**deny**用来指定拒绝符合条件的数据包，**permit**用来指定允许符合条件的数据包，**source**用来指定ACL规则匹配报文的源地址信息，**any**表示任意源地址。

traffic-filter { **inbound** | **outbound** }**acl**{ *acl-number* }命令用来在接口上配置基于ACL对报文进行过滤。

本示例中，主机A发送的流量到达RTA后，会匹配ACL2000中创建的规则rule deny source 192.168.1.0 0.0.0.255

，因而将被拒绝继续转发到Internet。主机B发送的流量不匹配任何规则，所以会被RTA正常转发到Internet。

配置确认

```
[RTA]display acl 2000
Basic ACL 2000, 1 rule
Acl's step is 5
 rule 5 deny source 192.168.1.0 0.0.0.255
```

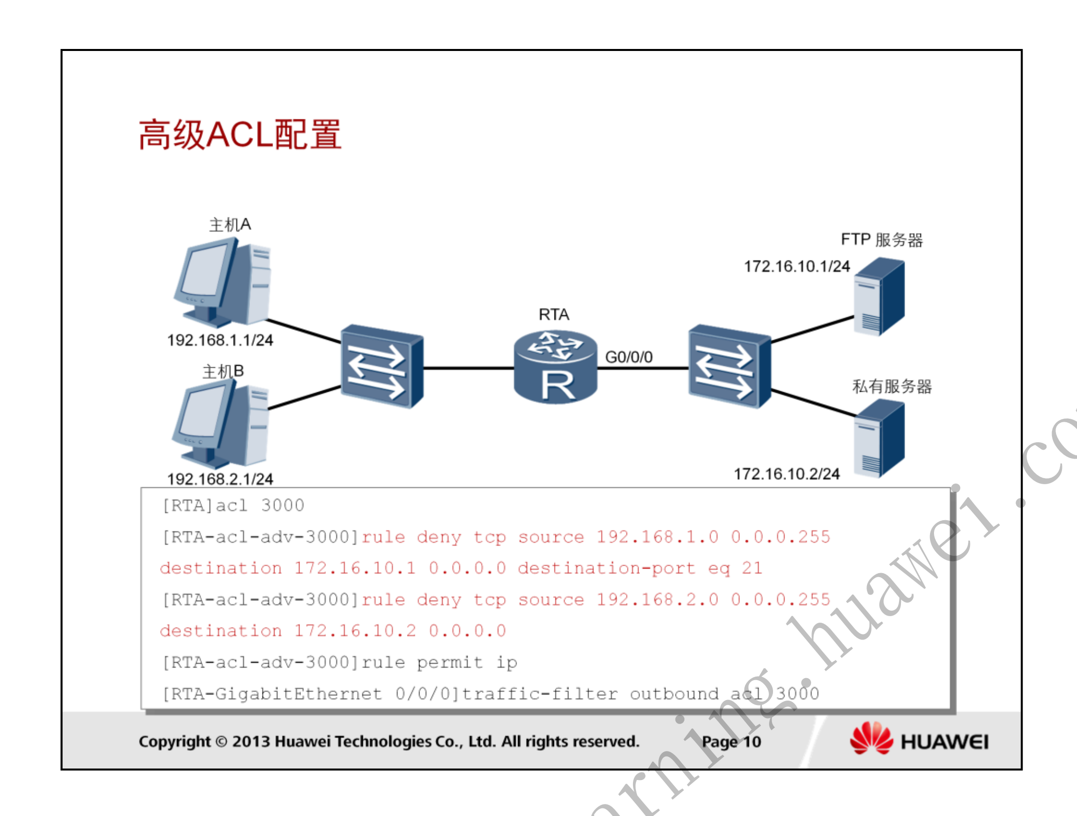
```
[RTA]display  traffic-filter applied-record
-----------------------------------------------------------
Interface                    Direction  AppliedRecord
-----------------------------------------------------------
GigabitEthernet0/0/0         outbound   acl 2000
-----------------------------------------------------------
```

 Page 9 

执行**display acl** <*acl-number*>命令可以验证配置的基本ACL。

本例中，所配置的ACL只有一条规则，即拒绝源IP地址在192.168.1.0/24范围的所有IP报文。

执行**display traffic-filter applied-record**命令可以查看设备上所有基于ACL进行报文过滤的应用信息，这些信息可以帮助用户了解报文过滤的配置情况并核对其是否正确，同时也有助于进行相关的故障诊断与排查。



基本ACL可以依据源IP地址进行报文过滤，而高级ACL能够依据源/目的IP地址、源/目的端口号、网络层及传输层协议以及IP流量分类和TCP标记值等各种参数（SYN|ACK|FIN等）进行报文过滤。

本示例中，RTA上定义了高级ACL3000，其中第一条规则“rule deny tcp source 192.168.1.0 0.0.0.255 destination 172.16.10.1 0.0.0.0 destination-port eq 21”用于限制源地址范围是192.168.1.0/24，目的IP地址为172.16.10.1，目的端口号为21的所有TCP报文；第二条规则“rule deny tcp source 192.168.2.0 0.0.0.255 destination 172.16.10.2 0.0.0.0”用于限制源地址范围是192.168.2.0/24，目的地址是172.16.10.2的所有TCP报文；第三条规则“rule permit ip”用于匹配所有IP报文，并对报文执行允许动作。

配置验证

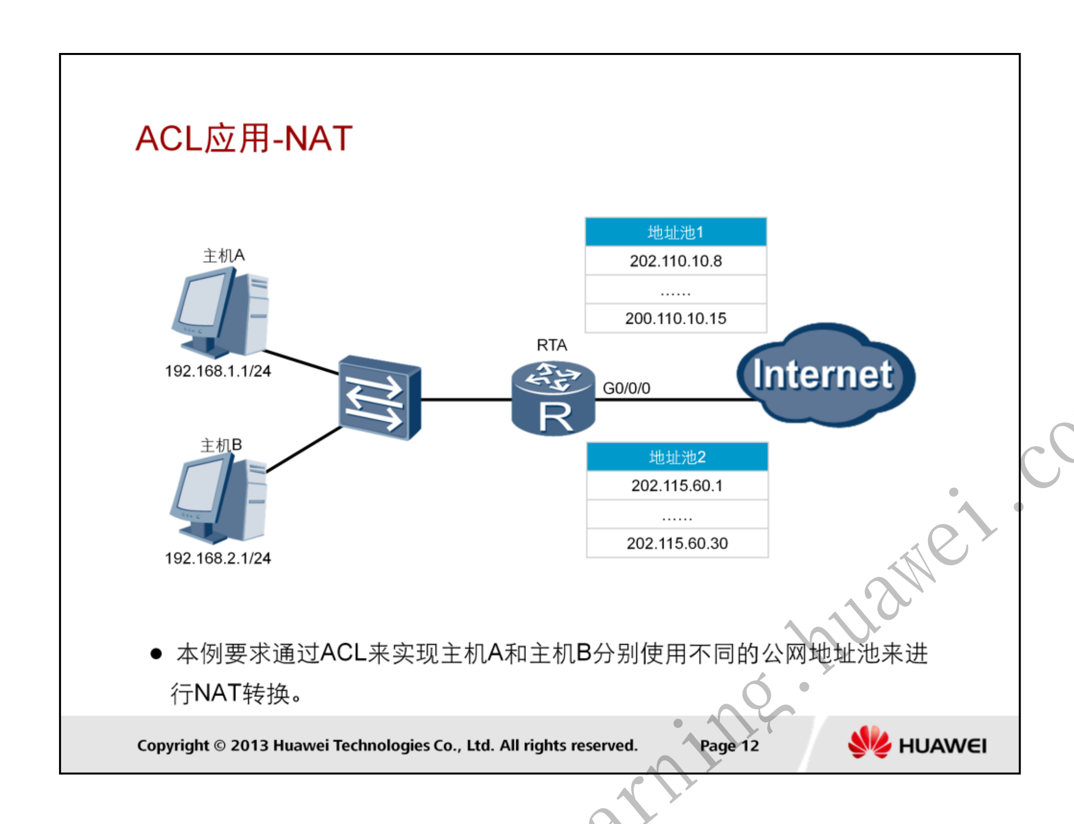
```
[RTA]display acl 3000
Advanced ACL 3000, 3 rules
Acl's step is 5
rule 5 deny tcp source 192.168.1.0 0.0.0.255 destination 172.16.10.1 0
destination-port eq ftp
rule 10 deny tcp source 192.168.2.0 0.0.0.255 destination 172.16.10.2
0
rule 15 permit ip
```

```
[RTA]display  traffic-filter applied-record
-----------------------------------------------------------
Interface                    Direction  AppliedRecord
-----------------------------------------------------------
GigabitEthernet0/0/0         outbound   acl 3000
-----------------------------------------------------------
```




执行**display acl** *<acl-number>*命令可以验证配置的高级ACL。

显示信息表明：RTA上一共配置了3条高级ACL规则。第一条规则用于拒绝来自源IP地址192.168.1.0/24，目的IP地址为172.16.10.1，目的端口为21（FTP）的TCP报文；第二条规则用于拒绝来自源IP地址192.168.2.0/24，目的IP地址为172.16.10.2的所有TCP报文；第三条规则允许所有IP报文通过。



ACL还可用于网络地址转换操作，以便在存在多个地址池的情况下，确定哪些内网地址是通过哪些特定外网地址池进行地址转换的。例如，某企业网络作为客户连接到多个服务供应商网络，企业网络的内部用户位于不同的网段/子网，他们期望分别通过某个特定的地址组进行地址转换来实现报文转发。这种情况极有可能发生在连接不同服务供应商网络的路由器上行端口。

本示例中，要求192.168.1.0/24中的主机使用地址池1中的公网地址进行地址转换，而192.168.2.0/24中的主机使用地址池2中的公网地址进行地址转换。

ACL应用-NAT

```
[RTA]nat address-group 1 202.110.10.8 202.110.10.15
[RTA]nat address-group 2 202.115.60.1 202.115.60.30
[RTA]acl 2000
[RTA-acl-basic-2000]rule permit source 192.168.1.0 0.0.0.255
[RTA-acl-basic-2000]acl 2001
[RTA-acl-basic-2001]rule permit source 192.168.2.0 0.0.0.255
[RTA-acl-basic-2001]interface GigabitEthernet0/0/0
[RTA-GigabitEthernet0/0/0]nat outbound 2000 address-group 1
[RTA-GigabitEthernet0/0/0]nat outbound 2001 address-group 2
```




执行**nat outbound** *<acl-number>* **address-group** *<address-group number>*命令，可以将NAT与ACL绑定。

本示例中，私网192.168.1.0/24将使用地址池220.110.10.8-220.110.10.15进行地址转换，私网192.168.2.0/24将使用地址池202.115.60.1-202.115.60.30进行地址转换。



1.高级ACL可以基于源/目的IP地址，源/目的端口号，协议类型以及IP流量分类和TCP标记值（SYN|ACK|FIN等）等参数来定义规则。


谢谢
www.huawei.com


AAA
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

AAA是Authentication（认证）、Authorization（授权）和Accounting（计费）的简称，它提供了认证、授权、计费三种安全功能。AAA可以通过多种协议来实现，目前华为设备支持基于RADIUS（Remote Authentication Dial-In User Service）协议或HWTACACS（Huawei Terminal Access Controller Access Control System）协议来实现AAA。



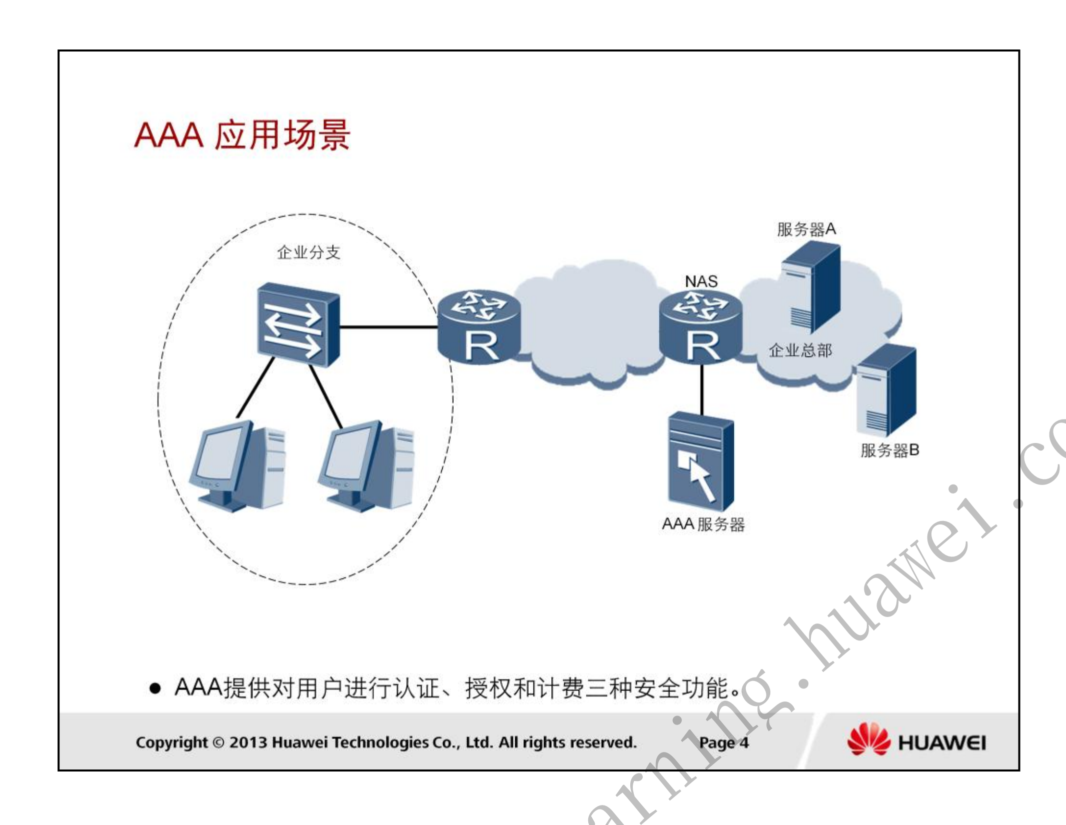


学习目标

学完本课程后，您应该能：

- 掌握AAA的基本概念
- 掌握AAA认证和授权的配置



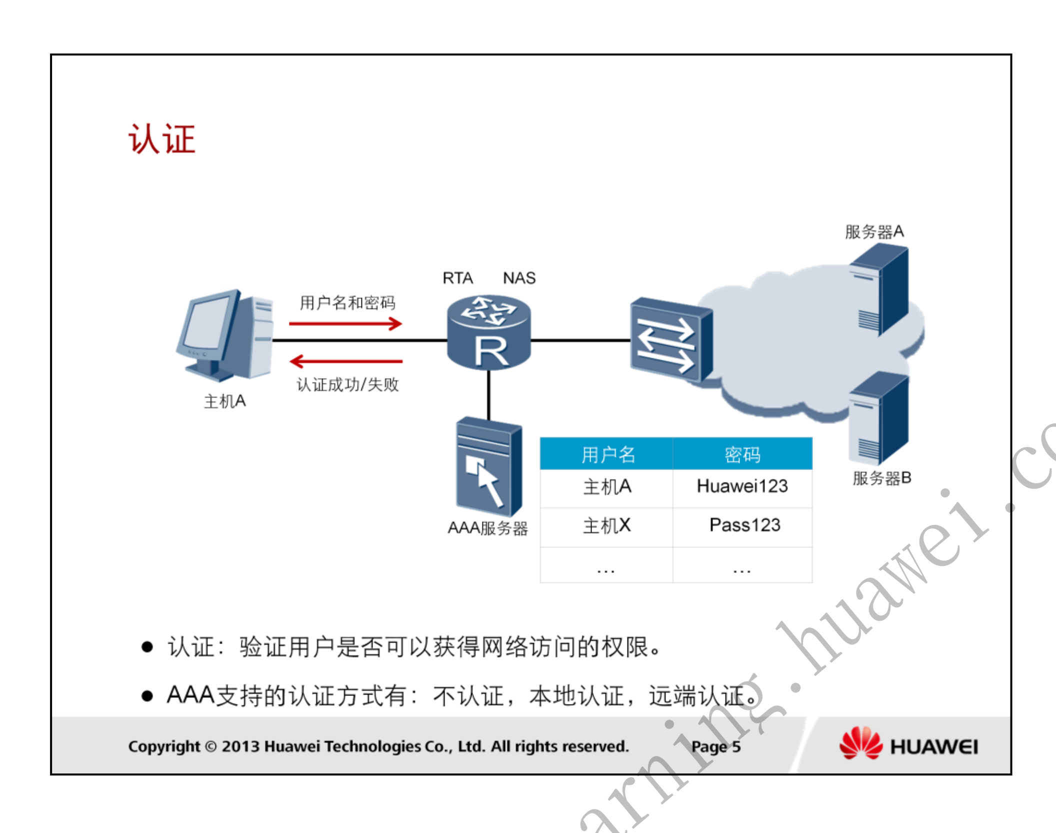


AAA是一种提供认证、授权和计费的安全技术。该技术可以用于验证用户帐户是否合法，授权用户可以访问的服务，并记录用户使用网络资源的情况。

例如，企业总部需要对服务器的资源访问进行控制，只有通过认证的用户才能访问特定的资源，并对用户使用资源的情况进行记录。在这种场景下，可以按照如图所示的方案进行AAA部署，NAS为网络接入服务器，负责集中收集和管理用户的访问请求。

AAA服务器表示远端的Radius或HWTACACS服务器，负责制定认证、授权和计费方案。如果企业分支的员工希望访问总部的服务器，远端的Radius或HWTACACS服务器会要求员工发送正确的用户名和密码，之后会进行验证，通过后则执行相关的授权策略，接下来，该员工就可以访问特定的服务器了。如果还需要记录员工访问网络资源的行为，网络管理员还可以在Radius或HWTACACS服务器上配置计费方案。

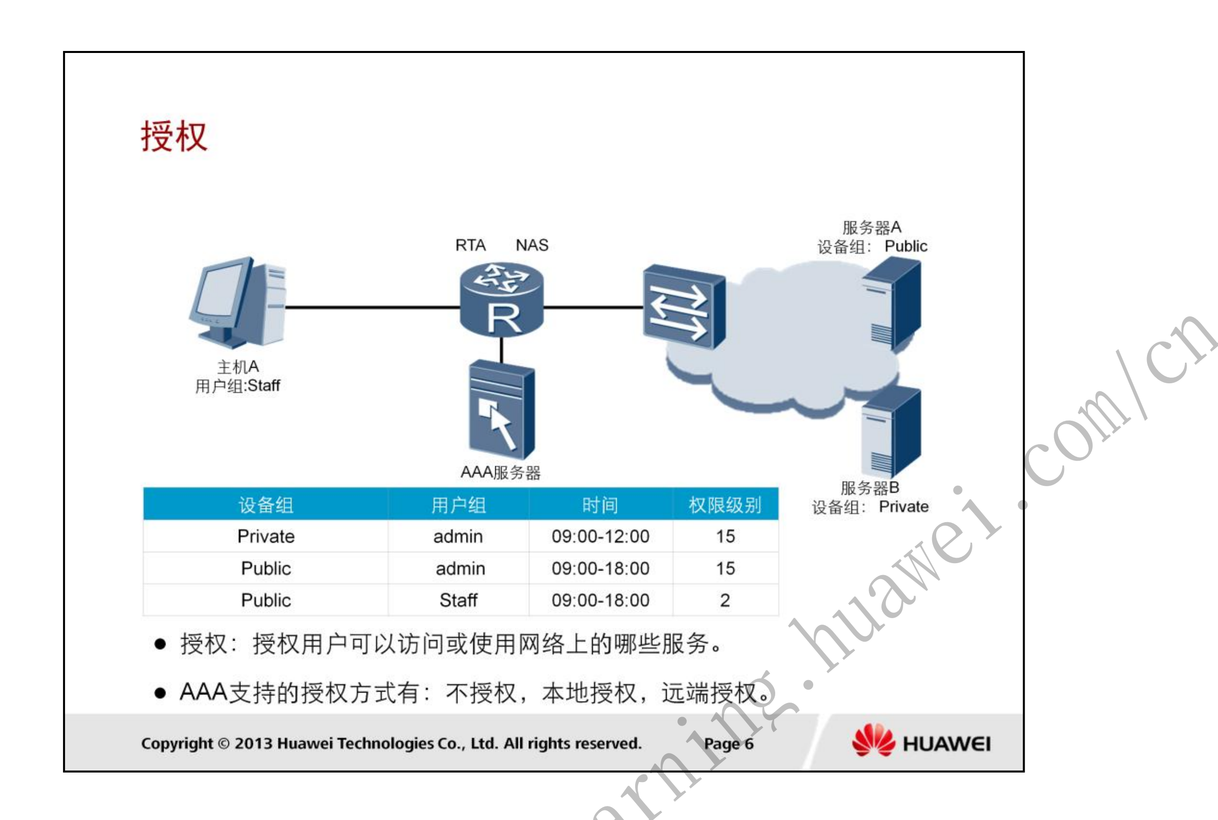
目前，ARG3系列路由器只支持配置认证和授权。



AAA支持三种认证方式:

1. 不认证：完全信任用户，不对用户身份进行合法性检查。鉴于安全考虑，这种认证方式很少被采用。
2. 本地认证：将本地用户信息（包括用户名、密码和各种属性）配置在NAS上。本地认证的优点是处理速度快、运营成本低；缺点是存储信息量受设备硬件条件限制。
3. 远端认证：将用户信息（包括用户名、密码和各种属性）配置在认证服务器上。AAA支持通过RADIUS协议或HWTACACS协议进行远端认证。NAS作为客户端，与RADIUS服务器或HWTACACS服务器进行通信。

如果一个认证方案采用多种认证方式，这些认证方式按配置顺序生效。比如，先配置了远端认证，随后配置了本地认证，那么在远端认证服务器无响应时，会转入本地认证方式。如果只在本地设备上配置了登录账号，没有在远端服务器上配置，AR2200认为账号没有通过远端认证，不再进行本地认证。

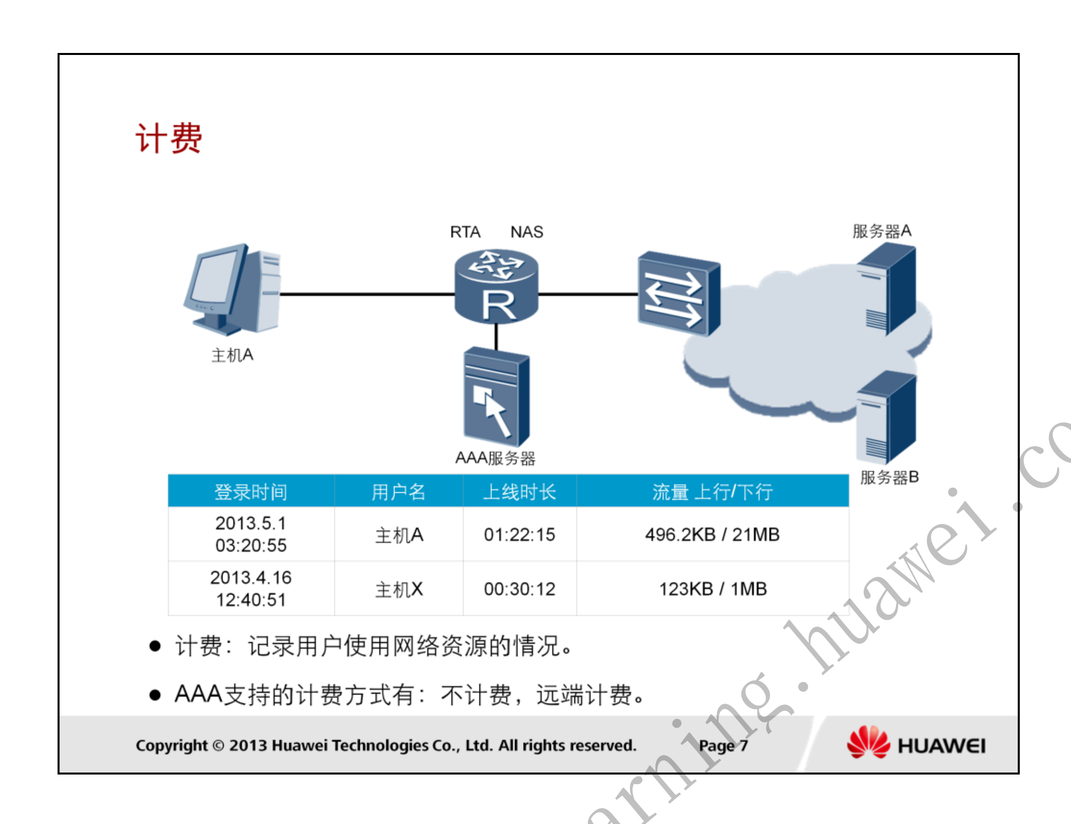


设备组	用户组	时间	权限级别
Private	admin	09:00-12:00	15
Public	admin	09:00-18:00	15
Public	Staff	09:00-18:00	2

AAA授权功能赋予用户访问的特定网络或设备的权限。AAA支持以下授权方式：

1. 不授权：不对用户进行授权处理。
2. 本地授权：根据NAS上配置的本地用户账号的相关属性进行授权。
3. 远端授权：HWTACACS授权，使用TACACS服务器对用户授权。RADIUS授权，对通过RADIUS服务器认证的用户授权。RADIUS协议的认证和授权是绑定在一起的，不能单独使用RADIUS进行授权。

如果在一个授权方案中使用多种授权方式，这些授权方式按照配置顺序生效。不授权方式最后生效。

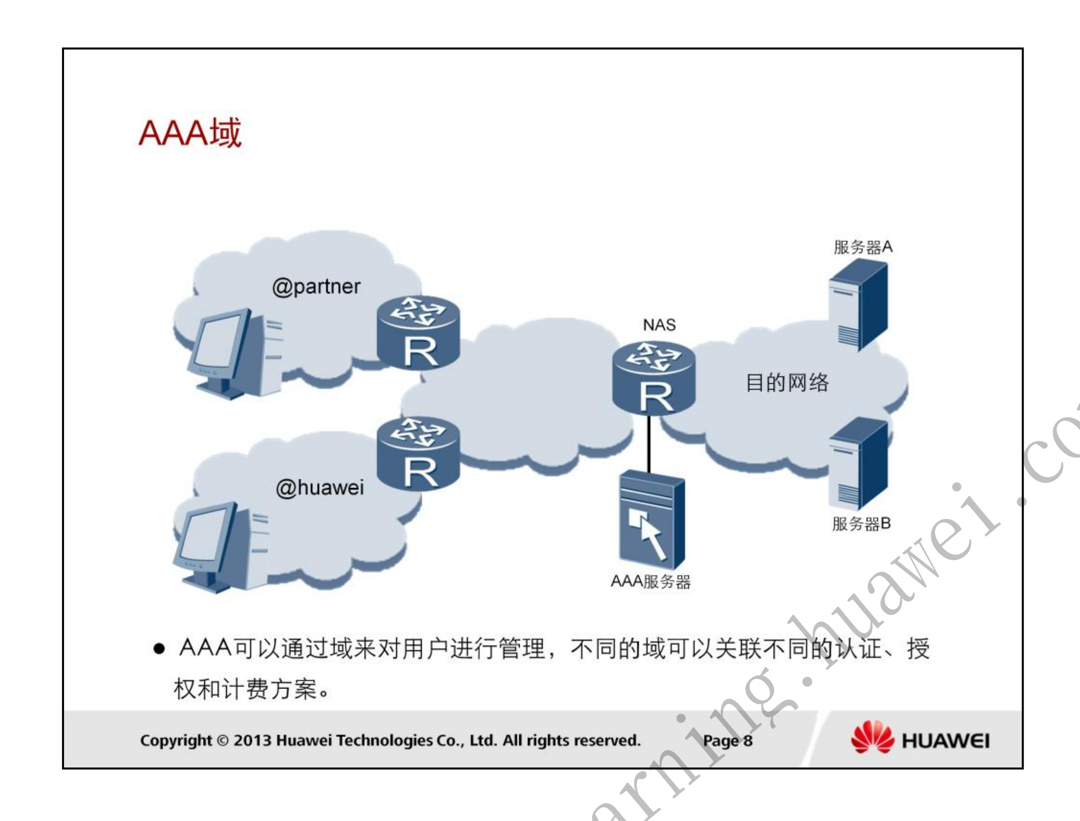


登录时间	用户名	上线时长	流量 上行/下行
2013.5.1 03:20:55	主机A	01:22:15	496.2KB / 21MB
2013.4.16 12:40:51	主机X	00:30:12	123KB / 1MB

计费功能用于监控授权用户的网络行为和网络资源的使用情况。AAA支持以下两种计费方式：

1. 不计费：为用户提供免费上网服务，不产生相关活动日志。
2. 远端计费：通过RADIUS服务器或HWTACACS服务器进行远端计费。RADIUS服务器或HWTACACS服务器具备充足的储存空间，可以储存各授权用户的网络访问活动日志，支持计费功能。

本示例中展示了用户计费日志中记录的典型信息。

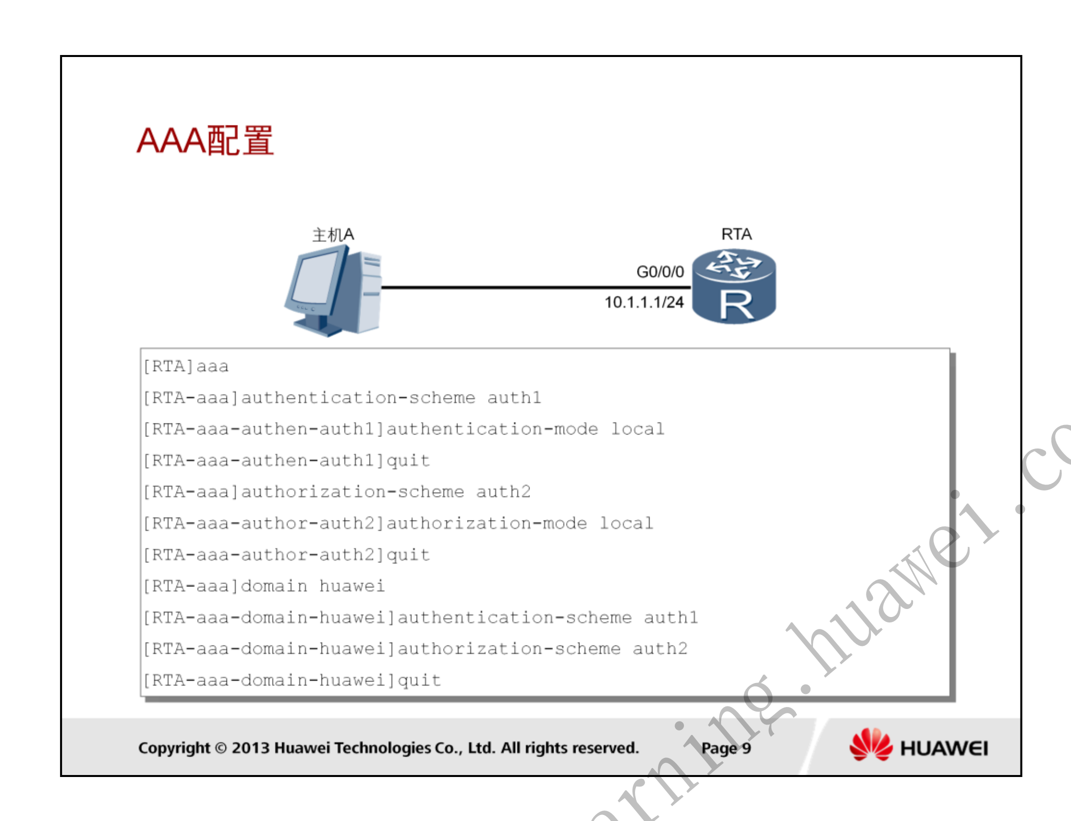


设备基于域来对用户进行管理，每个域都可以配置不同的认证、授权和计费方案，用于对该域下的用户进行认证、授权和计费。每个用户都属于某一个域。用户属于哪个域是由用户名中的域名分隔符@后的字符串决定。例如，如果用户名是user@huawei，则用户属于huawei域。如果用户名后不带有@，则用户属于系统缺省域default。

ARG3系列路由设备支持两种缺省域：

1. default域为普通用户的缺省域。
2. default_admin域为管理用户的缺省域。

用户可以修改但不能删除这两个缺省域。默认情况下，设备最多支持32个域，包括两个缺省域。



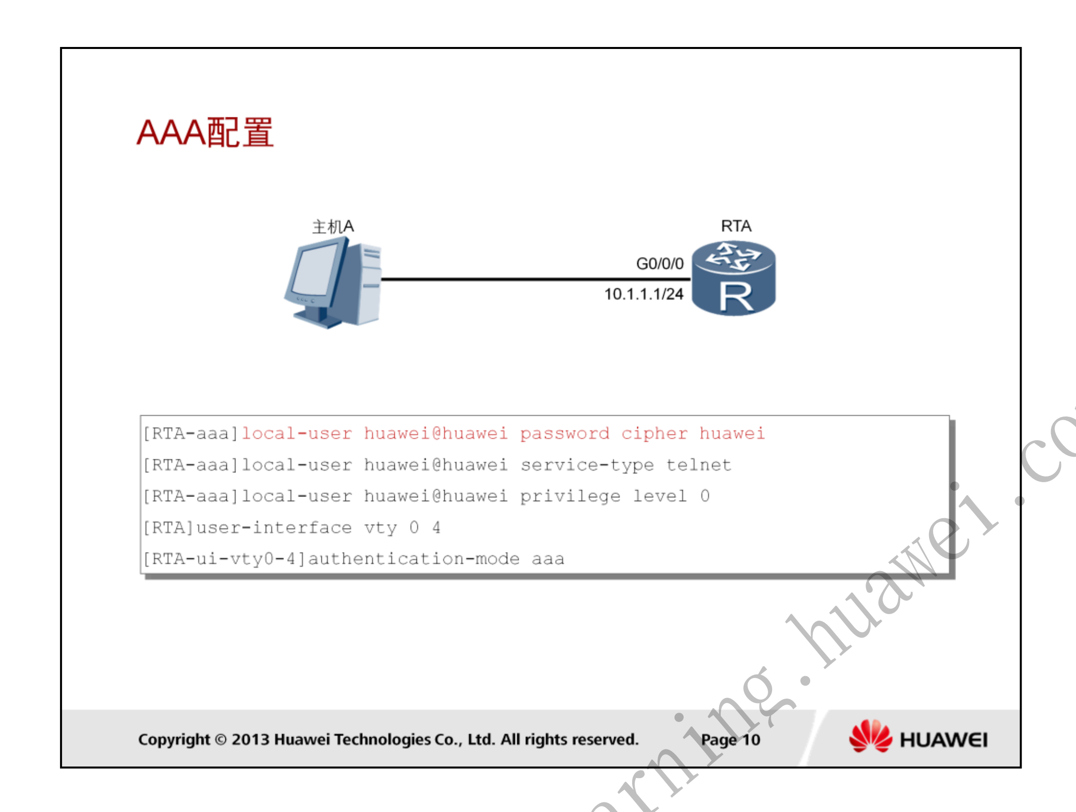
authentication-scheme *authentication-scheme-name*命令用来配置域的认证方案。缺省情况下，域使用名为“default”的认证方案。

authentication-mode { **hwtacacs** | **radius** | **local** }命令用来配置认证方式，**local**指定认证模方式为本地认证。缺省情况下，认证方式为本地认证。

authorization-scheme *authorization-scheme-name*命令用来配置域的授权方案。缺省情况下，域下没有绑定授权方案。

authorization-mode { [**hwtacacs** | **if-authenticated** | **local**] * [**none**] }命令用来配置当前授权方案使用的授权方式。缺省情况下，授权模式为本地授权方式。

domain *domain-name* 命令用来创建域，并进入AAA域视图。



local-user *user-name* **password cipher** *password*命令用来创建本地用户，并配置本地用户的密码。如果用户名中带域名分隔符，如@，则认为@前面的部分是用户名，后面部分是域名。如果没有@，则整个字符串为用户名，域为默认域。

local-user *user-name* **privilege level** *level*命令用来指定本地用户的优先级。

配置验证

```
[RTA]display domain name huawei
  Domain-name                      : huawei
  Domain-state                     : Active
  Authentication-scheme-name       : auth1
  Accounting-scheme-name           : default
  Authorization-scheme-name        : auth2
  Service-scheme-name              : -
  RADIUS-server-template           : -
  HWTACACS-server-template         : -
  User-group                       : -
```

- AAA中，每个域都会与相应的认证授权和计费方案相关联。

 Page 11



display domain [**name** *domain-name*]命令用来查看域的配置信息。Domain-state为Active表示激活状态。Authentication-scheme-name表示域使用的认证方案为auth1。缺省情况下，域使用系统自带的default认证方案。Authorization-scheme-name表示域使用的授权方案为auth2。



总结

- ARG3系列路由器上支持配置哪些AAA方案?
- 如果在ARG3系列路由器上创建用户时，没有关联自定义的域，则该用户属于哪个域?

 Page 12 

1. ARG3系列路由器上支持配置认证方案和授权方案，计费方案需要配置在HWTACACS或RADIUS服务器上。
2. 如果创建用户时未指定用户所属的域，用户会自动关联缺省域default。

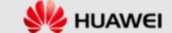

谢谢
www.huawei.com


IPSec VPN原理与配置
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

企业对网络安全性的需求日益提升，而传统的TCP/IP协议缺乏有效的安全认证和保密机制。IPSec（Internet Protocol Security）作为一种开放标准的安全框架结构，可以用来保证IP数据报文在网络上传输的机密性、完整性和防重放。

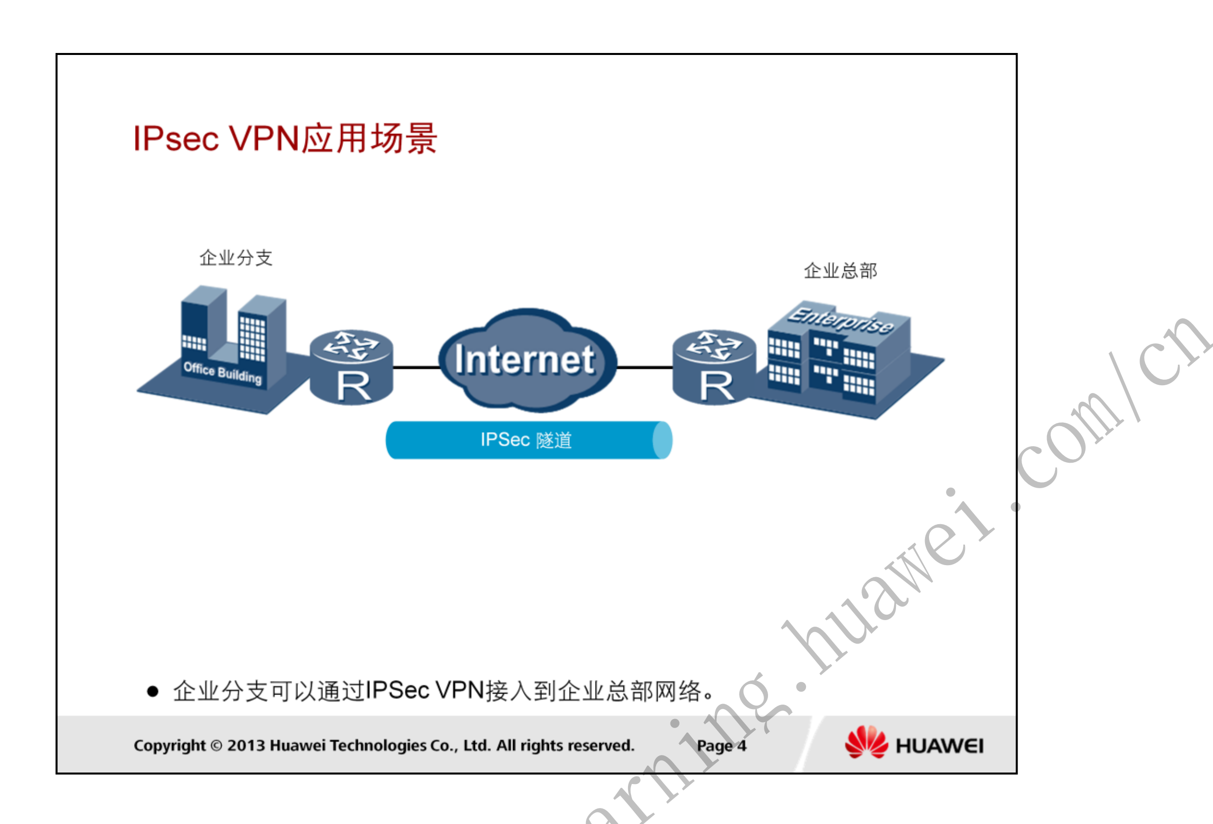




学习目标

学完本课程后，您应该能：

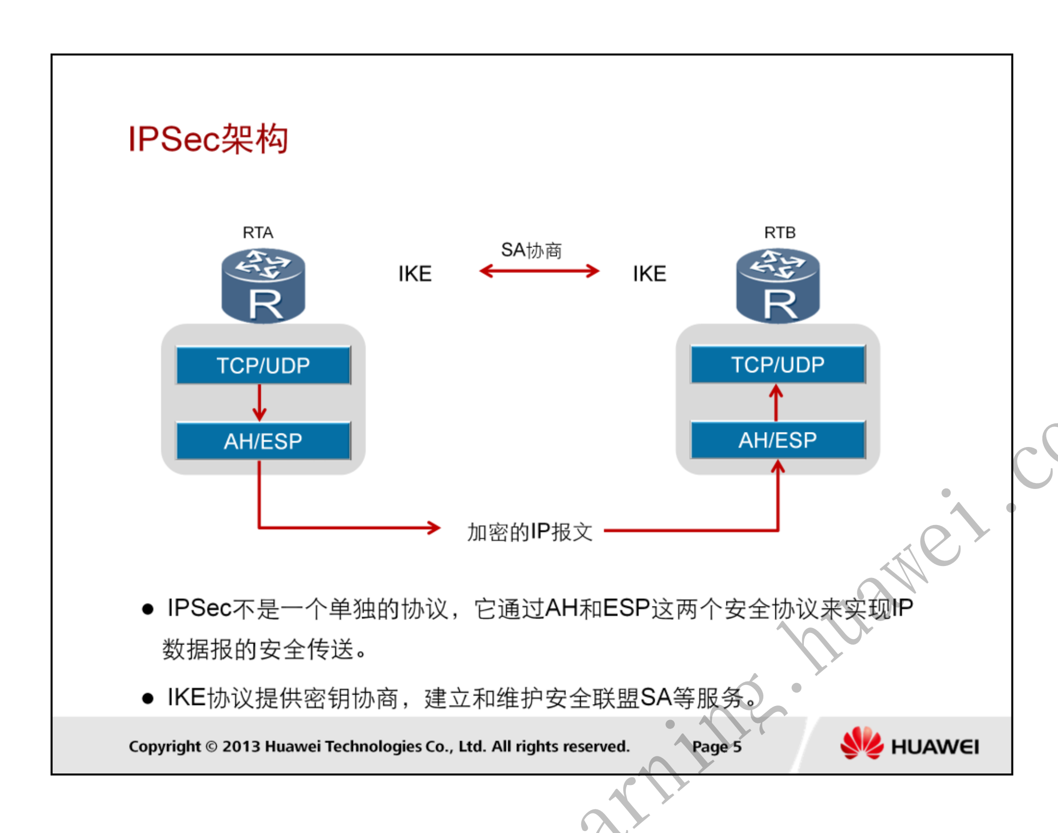
- 掌握IPSec VPN的基本概念
- 掌握IPSec VPN的基本配置



IPSec是IETF定义的一个协议组。通信双方在IP层通过加密、完整性校验、数据源认证等方式，保证了IP数据报文在网络上传输的机密性、完整性和防重放。

1. 机密性（Confidentiality）指对用户数据进行加密保护，用密文的形式传送数据。
2. 完整性（Data integrity）指对接收的数据进行认证，以判定报文是否被篡改。
3. 防重放（Anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。

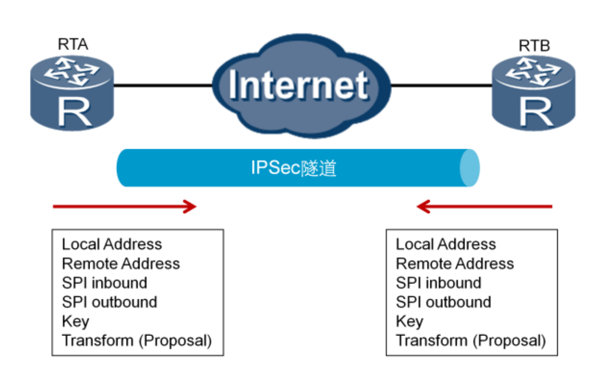
企业远程分支机构可以通过使用IPSec VPN建立安全传输通道，接入到企业总部网络。



IPSec VPN体系结构主要由AH（Authentication Header）、ESP（Encapsulating Security Payload）和IKE（Internet Key Exchange）协议套件组成。

1. AH协议：主要提供的功能有数据源验证、数据完整性校验和防报文重放功能。然而，AH并不加密所保护的数据报。
2. ESP协议：提供AH协议的所有功能外（但其数据完整性校验不包括IP头），还可提供对IP报文的加密功能。
3. IKE协议：用于自动协商AH和ESP所使用的密码算法。

安全联盟SA



- 安全联盟定义了IPSec对等体间将使用的数据封装模式、认证和加密算法、密钥等参数。
- 安全联盟是单向的，两个对等体之间的双向通信，至少需要两个SA。

 Page 6

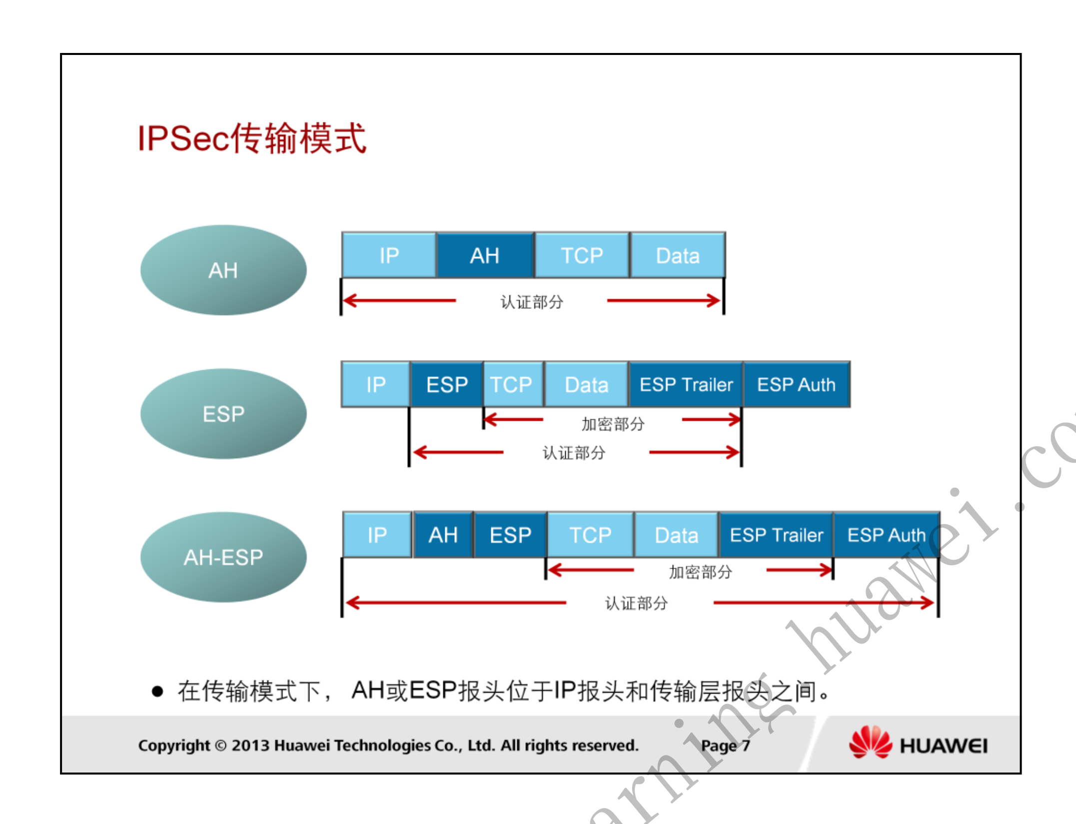


SA（Security Association）安全联盟定义了IPSec通信对等体间将使用的数据封装模式、认证和加密算法、秘钥等参数。SA是单向的，两个对等体之间的双向通信，至少需要两个SA。如果两个对等体希望同时使用AH和ESP安全协议来进行通信，则对等体针对每一种安全协议都需要协商一对SA。

SA由一个三元组来唯一标识，这个三元组包括安全参数索引SPI（Security Parameter Index）、目的IP地址、安全协议（AH或ESP）。

建立SA的方式有以下两种：

1. 手工方式：安全联盟所需的全部信息都必须手工配置。手工方式建立安全联盟比较复杂，但优点是可以不依赖IKE而单独实现IPSec功能。当对等体设备数量较少时，或是在小型静态环境中，手工配置SA是可行的。
2. IKE动态协商方式：只需要通信对等体间配置好IKE协商参数，由IKE自动协商来创建和维护SA。动态协商方式建立安全联盟相对简单些。对于中、大型的动态网络环境中，推荐使用IKE协商建立SA。



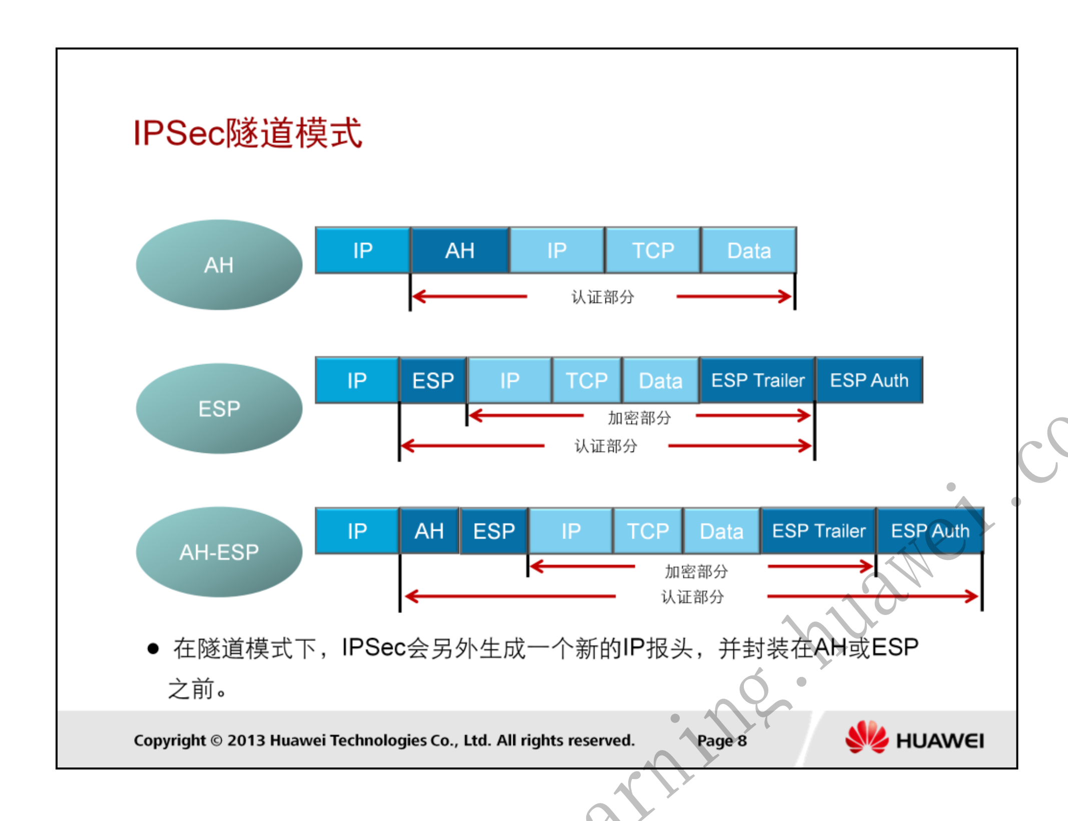
IPSec协议有两种封装模式：传输模式和隧道模式。

传输模式中，在IP报文头和高层协议之间插入AH或ESP头。传输模式中的AH或ESP主要对上层协议数据提供保护。

传输模式中的AH：在IP头部之后插入AH头，对整个IP数据包进行完整性校验。

传输模式中的ESP：在IP头部之后插入ESP头，在数据字段后插入尾部以及认证字段。对高层数据和ESP尾部进行加密，对IP数据包中的ESP报文头，高层数据和ESP尾部进行完整性校验。

传输模式中的AH+ESP：在IP头部之后插入AH和ESP头，在数据字段后插入尾部以及认证字段。对高层数据和ESP尾部进行加密，对整个IP数据包进行完整性校验。

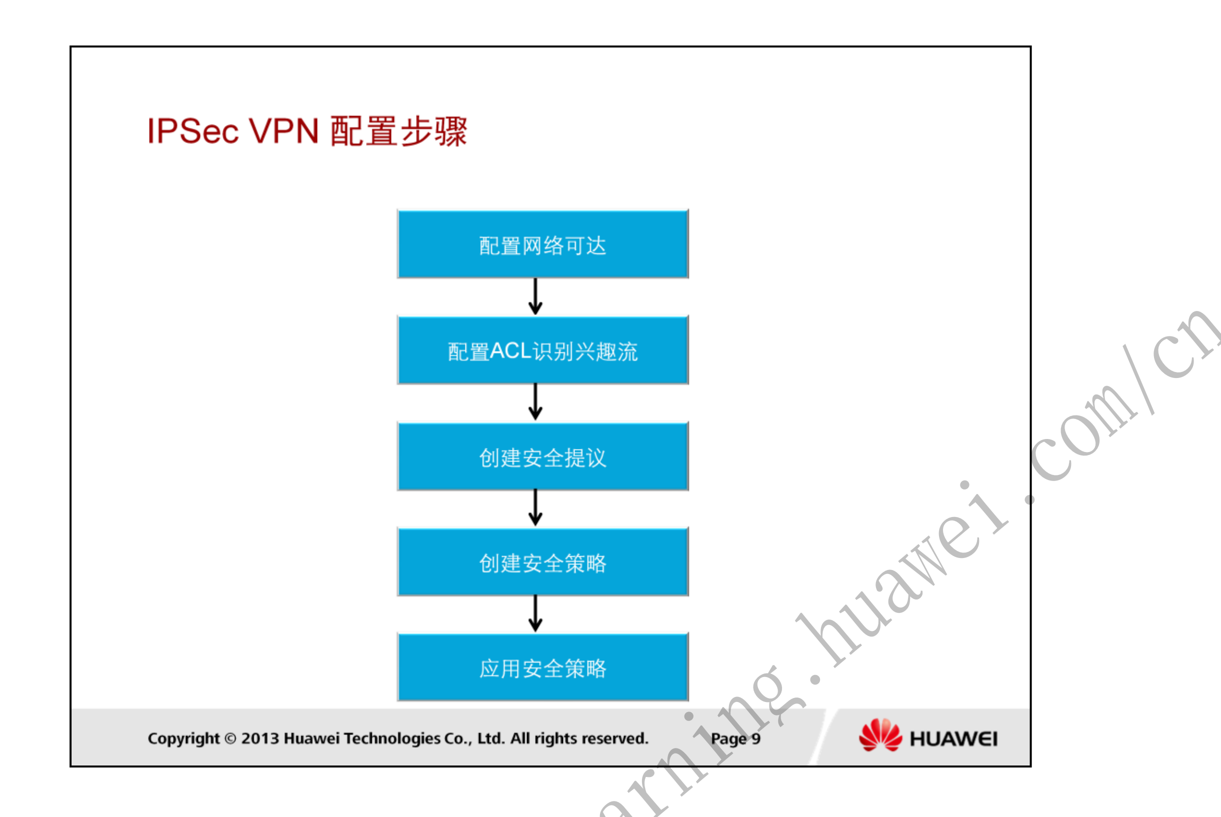


隧道模式中，AH或ESP头封装在原始IP报文头之前，并另外生成一个新的IP头封装到AH或ESP之前。隧道模式可以完全地对原始IP数据报进行认证和加密，而且，可以使用IPSec对等体的IP地址来隐藏客户机的IP地址。

隧道模式中的AH：对整个原始IP报文提供完整性检查和认证，认证功能优于ESP。但AH不提供加密功能，所以通常和ESP联合使用。

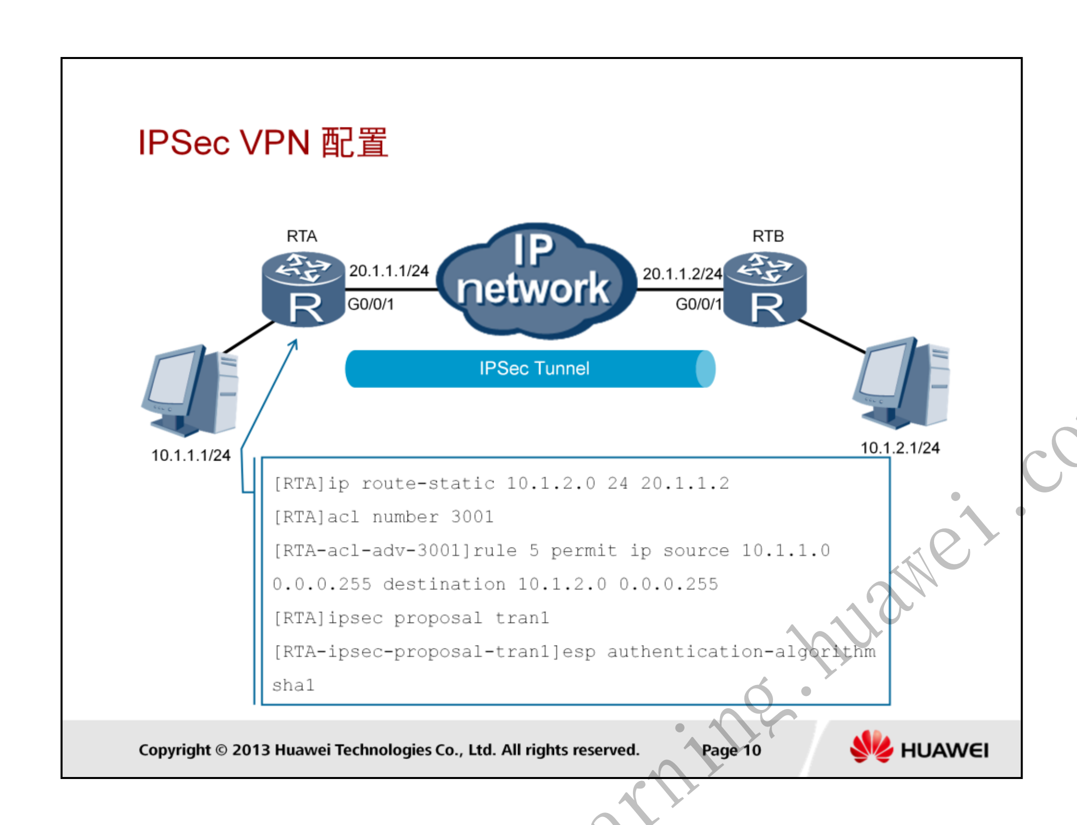
隧道模式中的ESP：对整个原始IP报文和ESP尾部进行加密，对ESP报文头，原始IP报文和ESP尾部进行完整性校验。

隧道模式中的AH+ESP：对整个原始IP报文和ESP尾部进行加密，对除新IP头之外的整个IP数据包进行完整性校验。



配置IPSec VPN的步骤如下:

1. 首先需要检查报文发送方和接收方之间的网络层可达性，确保双方只有建立IPSec VPN隧道才能进行IPSec通信。
2. 第二步是定义数据流。因为部分流量无需满足完整性和机密性要求，所以需要对流量进行过滤，选择出需要进行IPSec处理的兴趣流。可以通过配置ACL来定义和区分不同的数据流。
3. 第三步是配置IPSec安全提议。IPSec提议定义了保护数据流所用的安全协议、认证算法、加密算法和封装模式。安全协议包括AH和ESP，两者可以单独使用或一起使用。AH支持MD5和SHA-1认证算法；ESP支持两种认证算法（MD5和SHA-1）和三种加密算法（DES、3DES和AES）。为了能够正常传输数据流，安全隧道两端的对等体必须使用相同的安全协议、认证算法、加密算法和封装模式。如果要在两个安全网关之间建立IPSec隧道，建议将IPSec封装模式设置为隧道模式，以便隐藏通信使用的实际源IP地址和目的IP地址。
4. 第四步是配置IPSec安全策略。IPSec策略中会应用IPSec提议中定义的安全协议、认证算法、加密算法和封装模式。每一个IPSec安全策略都使用唯一的名称和序号来标识。IPSec策略可分成两类：手工建立SA的策略和IKE协商建立SA的策略。
5. 第五步是在一个接口上应用IPSec安全策略。



本示例中的IPSec VPN连接是通过配置静态路由建立的，下一跳指向RTB。需要配置两个方向的静态路由确保双向通信可达。建立一条高级ACL，用于确定哪些感兴趣流需要通过IPSec VPN隧道。高级ACL能够依据特定参数过滤流量，继而对流量执行丢弃、通过或保护操作。

执行**ipsec proposal**命令，可以创建IPSec提议并进入IPSec提议视图。配置IPSec策略时，必须引用IPSec提议来指定IPSec隧道两端使用的安全协议、加密算法、认证算法和封装模式。缺省情况下，使用**ipsec proposal**命令创建的IPSec提议采用ESP协议、DES加密算法、MD5认证算法和隧道封装模式。在IPSec提议视图下执行下列命令可以修改这些参数。

执行**transform [ah | ah-esp | esp]**命令，可以重新配置隧道采用的安全协议。

执行**encapsulation-mode {transport | tunnel }**命令，可以配置报文的封装模式。

执行**esp authentication-algorithm [md5 | sha1 | sha2-256 | sha2-384 | sha2-512]**命令，可以配置ESP协议使用的认证算法。

执行**esp encryption-algorithm [des | 3des | aes-128 | aes-192 | aes-256]**命令，可以配置ESP加密算法。

执行**ah authentication-algorithm [md5 | sha1 | sha2-256 | sha2-384 | sha2-512]**命令，可以配置AH协议使用的认证算法。

配置验证

```
[RTA]display ipsec proposal
 Number of proposals: 1
 IPSec proposal name: tran1
 Encapsulation mode: Tunnel
 Transform          : esp-new
 ESP protocol       : Authentication SHA1-HMAC-96
                      Encryption     DES
```

- IPSec VPN对等体配置的安全提议参数必须一致。



执行**display ipsec proposal [name <proposal-name>]**命令，可以查看IPSec提议中配置的参数。

Number of proposals字段显示的是已创建的IPSec提议的个数。

IPSec proposal name字段显示的是已创建IPSec提议的名称。

Encapsulation mode字段显示的指定提议当前使用的封装模式，其值可以为传输模式或隧道模式。

Transform字段显示的是IPSec所采用的安全协议，其值可以是AH、ESP或AH-ESP。

ESP protocol字段显示的是安全协议所使用的认证和加密算法。

IPSec VPN 配置

```
[RTA]ipsec  policy P1 10 manual
[RTA-ipsec-policy-manual-P1-10]security acl 3001
[RTA-ipsec-policy-manual-P1-10]proposal tran1
[RTA-ipsec-policy-manual-P1-10]tunnel remote 20.1.1.2
[RTA-ipsec-policy-manual-P1-10]tunnel local 20.1.1.1
[RTA-ipsec-policy-manual-P1-10]sa spi outbound esp 54321
[RTA-ipsec-policy-manual-P1-10]sa spi inbound esp 12345
[RTA-ipsec-policy-manual-P1-10]sa string-key outbound esp simple
huawei
[RTA-ipsec-policy-manual-P1-10]sa string-key inbound esp simple huawei
```

- 安全策略将要保护的数据流和安全提议进行绑定。



ipsec policy *policy-name seq-number*命令用来创建一条IPSec策略，并进入IPSec策略视图。安全策略是由*policy-name*和*seq-number*共同来确定的，多个具有相同*policy-name*的安全策略组成一个安全策略组。在一个安全策略组中最多可以设置16条安全策略，而*seq-number*越小的安全策略，优先级越高。在一个接口上应用了一个安全策略组，实际上是同时应用了安全策略组中所有的安全策略，这样能够对不同的数据流采用不同的安全策略进行保护。

IPSec策略除了指定策略的名称和序号外，还需要指定SA的建立方式。如果使用的是IKE协商，需要执行**ipsec-policy-template**命令配置指定参数。如果使用的是手工建立方式，所有参数都需要手工配置。本示例采用的是手工建立方式。

security acl *acl-number*命令用来指定IPSec策略所引用的访问控制列表。

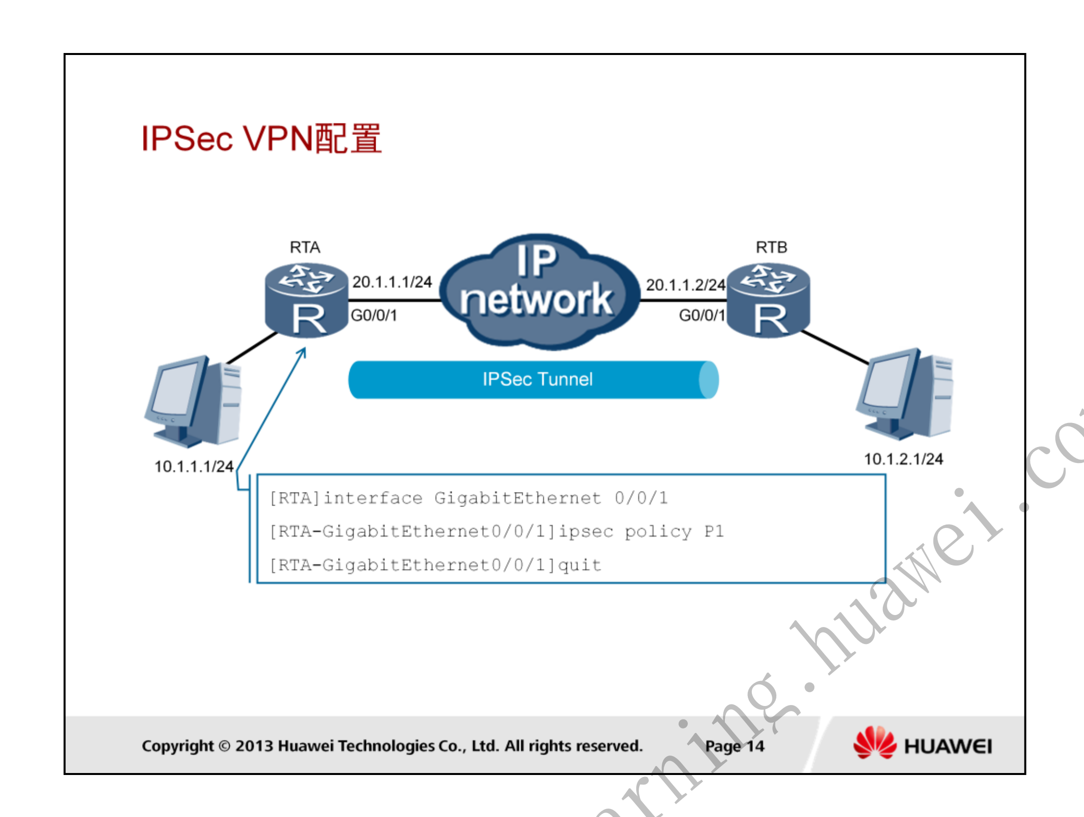
proposal *proposal-name*命令用来指定IPSec策略所引用的提议。

tunnel local { *ip-address* | *binding-interface* }命令用来配置安全隧道的本端地址。

tunnel remote *ip-address*命令用来设置安全隧道的对端地址。

sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*命令用来设置安全联盟的安全参数索引SPI。在配置安全联盟时，入方向和出方向安全联盟的安全参数索引都必须设置，并且本端的入方向安全联盟的SPI值必须和对端的出方向安全联盟的SPI值相同，而本端的出方向安全联盟的SPI值必须和对端的入方向安全联盟的SPI值相同。

sa string-key { inbound | outbound } { ah | esp } { simple | cipher } *string-key*命令用来设置安全联盟的认证密钥。入方向和出方向安全联盟的认证密钥都必须设置，并且本端的入方向安全联盟的密钥必须和对端的出方向安全联盟的密钥相同；同时，本端的出方向安全联盟密钥必须和对端的入方向安全联盟的密钥相同。



ipsec policy *policy-name*命令用来在接口上应用指定的安全策略组。手工方式配置的安全策略只能应用到一个接口。

配置验证

```
[RTA]display ipsec policy
===========================================
IPSec policy group: "P1"
Using interface: GigabitEthernet 0/0/1
===========================================
    Sequence number: 10
    Security data flow: 3001
    Tunnel local  address: 20.1.1.1
    Tunnel remote address: 20.1.1.2
    Qos pre-classify: Disable
    Proposal name:tran1
...
```


执行**display ipsec policy [brief | name** *policy-name* [*seq-number*]**]**命令，可以查看指定IPSec策略或所有IPSec策略。命令的显示信息中包括：策略名称、策略序号、提议名称、ACL、隧道的本端地址和隧道的远端地址等。

配置验证

```
……
Inbound ESP setting:
      ESP SPI: 12345 (0x3039)
      ESP string-key: huawei
      ESP encryption hex key:
      ESP authentication hex key:
   Outbound ESP setting:
      ESP SPI: 54321 (0xd431)
      ESP string-key: huawei
      ESP encryption hex key:
      ESP authentication hex key:
……
```

 Page 16



执行**display ipsec policy**命令，还可以查看出方向和入方向SA相关的参数。



总结

- 安全联盟的作用是什么？
- IPSec VPN将会对过滤后的感兴趣数据流如何操作？



1. SA（Security Association）安全联盟定义了IPSec通信对等体间将使用的数据封装模式、认证和加密算法、密钥等参数。
2. 经过IPSec过滤后的感兴趣数据流将会通过SA协商的各种参数进行处理并封装，之后通过IPSec隧道转发。


谢谢
www.huawei.com


GRE原理与配置
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

IPSec VPN用于在两个端点之间提供安全的IP通信，但只能加密并传播单播数据，无法加密和传输语音、视频、动态路由协议信息等组播数据流量。

通用路由封装协议GRE（Generic Routing Encapsulation）提供了将一种协议的报文封装在另一种协议报文中的机制，是一种隧道封装技术。GRE可以封装组播数据，并可以和IPSec结合使用，从而保证语音、视频等组播业务的安全。

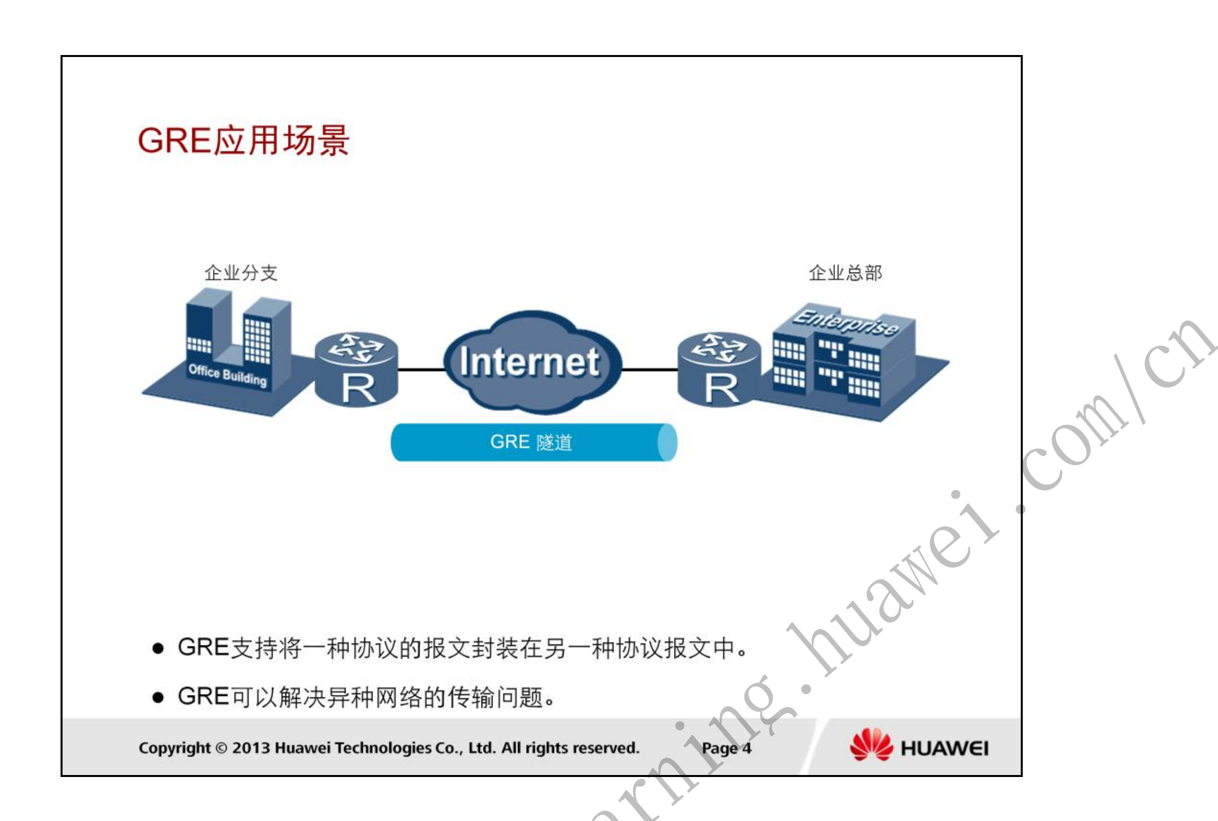




学习目标

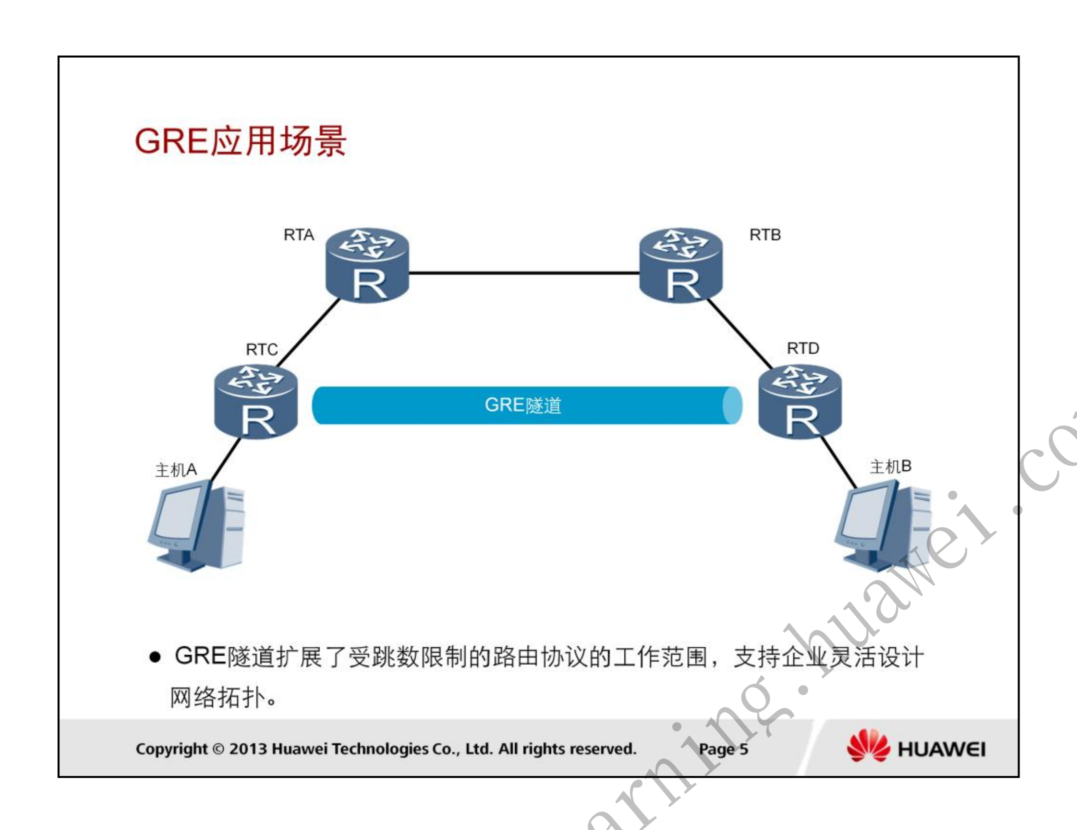
学完本课程后，您应该能：

- 掌握GRE的应用场景
- 掌握GRE的工作原理
- 掌握GRE over IPSec的配置

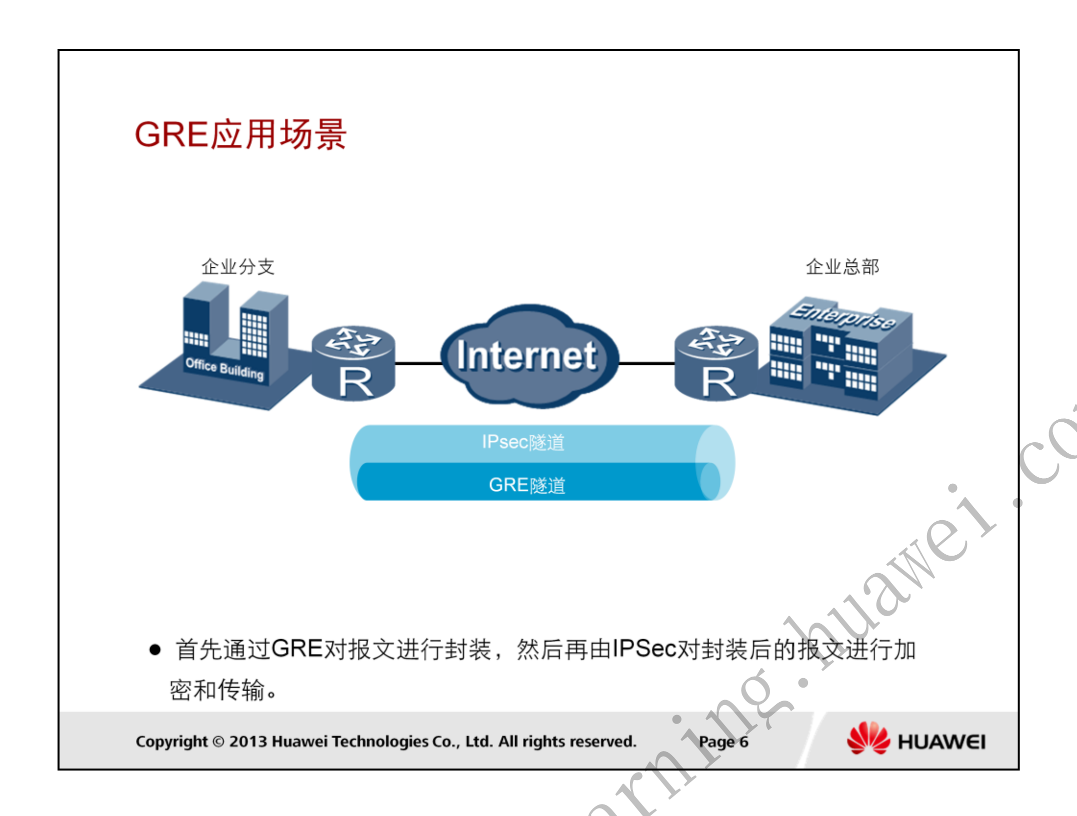


GRE用来对某些网络层协议如IPX（Internet Packet Exchange）的报文进行封装，使这些被封装的报文能够在另一网络层协议（如IP）中传输。GRE可以解决异种网络的传输问题。

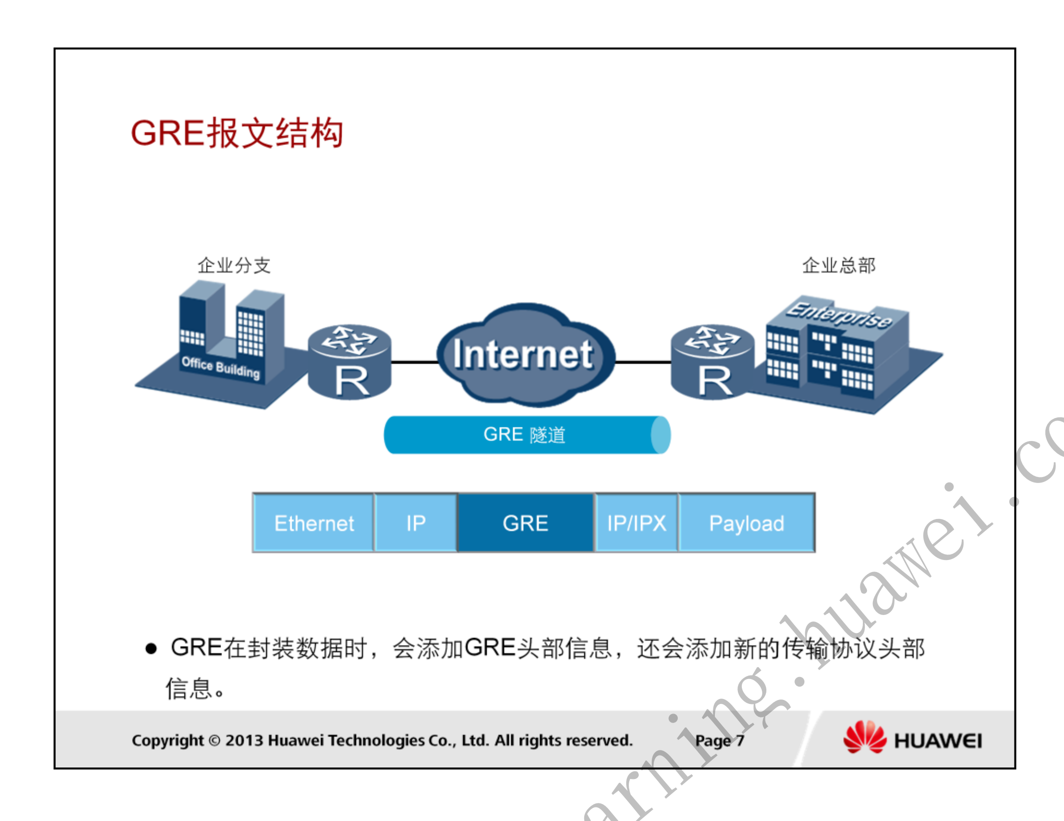
IPSec VPN技术可以创建一条跨越共享公网的隧道，从而实现私网互联。IPSec VPN能够安全传输IP报文，但是无法在隧道的两个端点之间运行RIP和OSPF等路由协议。GRE可以将路由协议信息封装在另一种协议报文（例如IP）中进行传输。



使用GRE可以克服IGP协议的一些局限性。例如，RIP路由协议是一种距离矢量路由协议，最大跳数为15。如果网络直径超过15，设备将无法通信。这种情况下，可以使用GRE技术在两个网络节点之间搭建隧道，隐藏它们之间的跳数，扩大网络的工作范围。



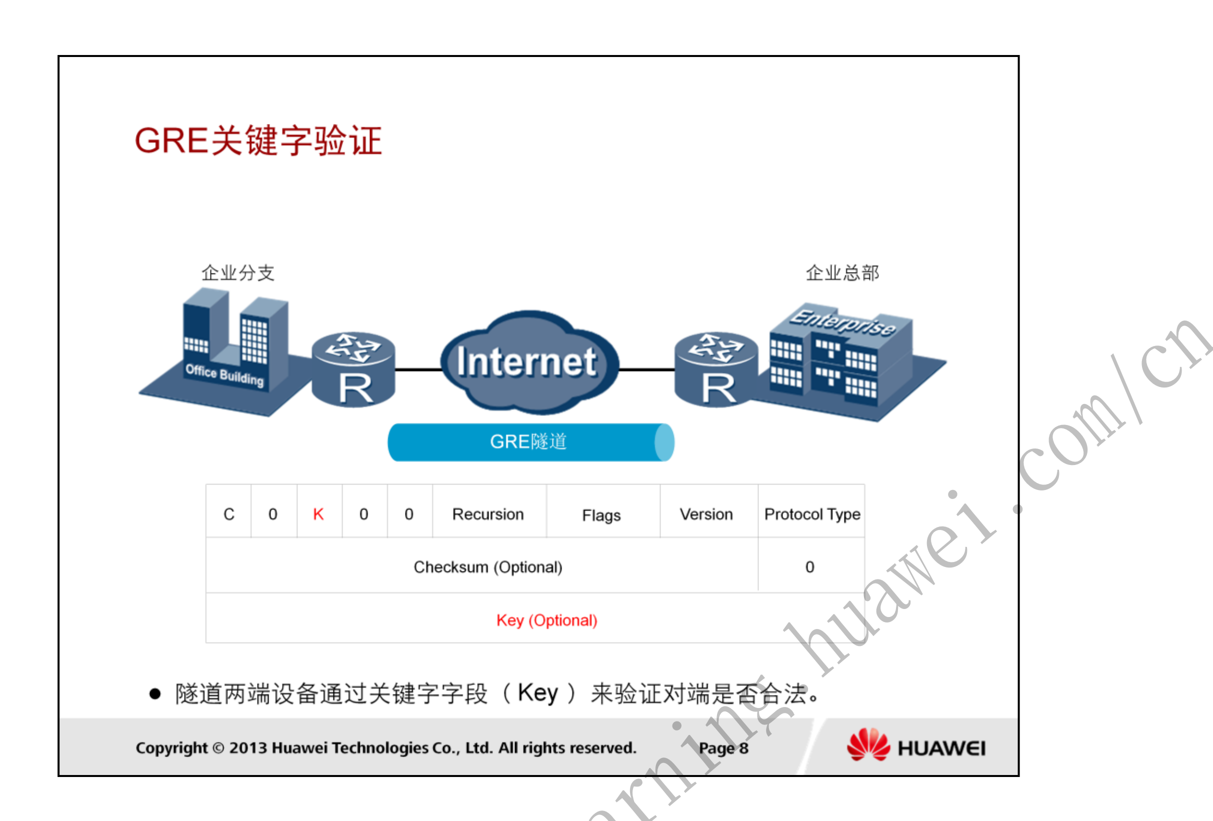
GRE本身并不支持加密，因而通过GRE隧道传输的流量是不加密的。将IPSec技术与GRE相结合，可以先建立GRE隧道对报文进行GRE封装，然后再建立IPSec隧道对报文进行加密，以保证报文传输的完整性和私密性。



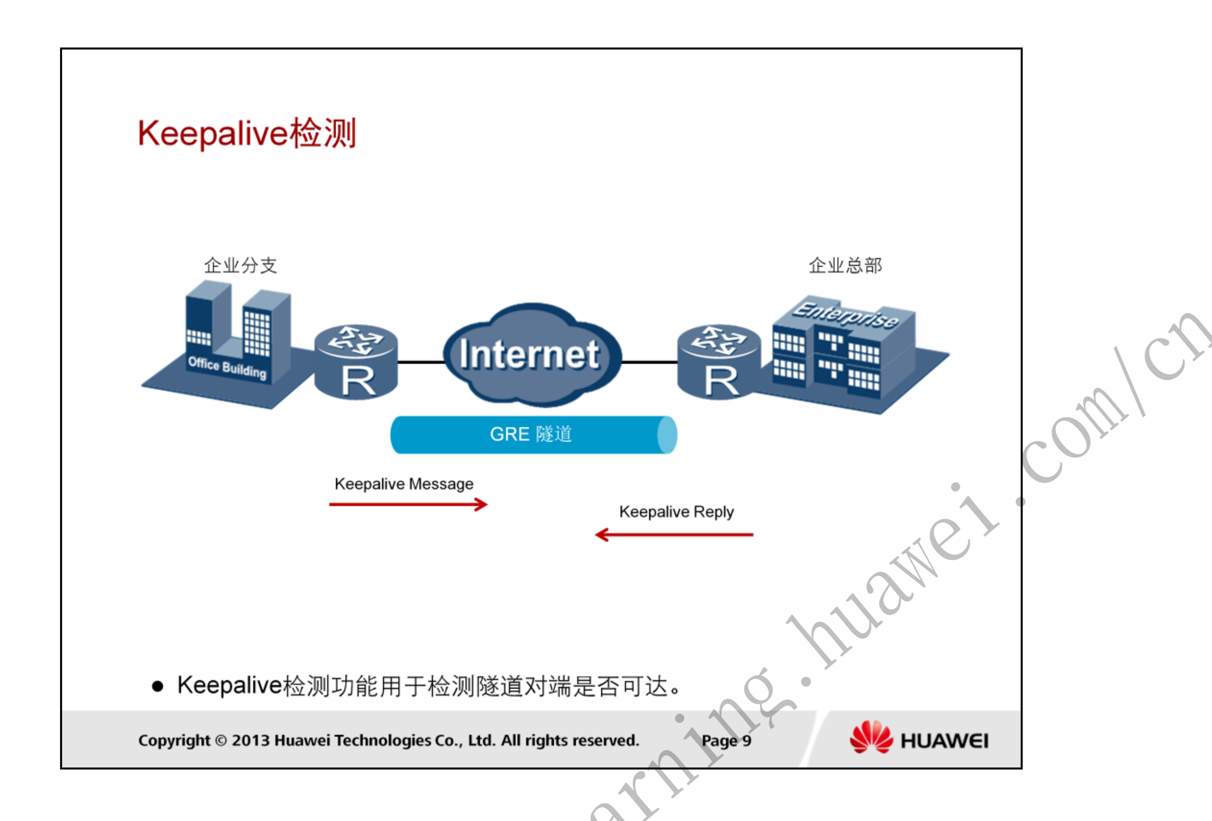
GRE封装报文时，封装前的报文称为净荷，封装前的报文协议称为乘客协议，然后GRE会封装GRE头部，GRE成为封装协议，也叫运载协议，最后负责对封装后的报文进行转发的协议称为传输协议。

GRE封装和解封装报文的过程如下:

1. 设备从连接私网的接口接收到报文后，检查报文头中的目的IP地址字段，在路由表查找出接口，如果发现出接口是隧道接口，则将报文发送给隧道模块进行处理。
2. 隧道模块接收到报文后首先根据乘客协议的类型和当前GRE隧道配置的校验和参数，对报文进行GRE封装，即添加GRE报文头。
3. 然后，设备给报文添加传输协议报文头，即IP报文头。该IP报文头的源地址就是隧道源地址，目的地址就是隧道目的地址。
4. 最后，设备根据新添加的IP报文头目的地址，在路由表中查找相应的出接口，并发送报文。之后，封装后的报文将在公网中传输。
5. 接收端设备从连接公网的接口收到报文后，首先分析IP报文头，如果发现协议类型字段的值为47，表示协议为GRE，于是出接口将报文交给GRE模块处理。GRE模块去掉IP报文头和GRE报文头，并根据GRE报文头的协议类型字段，发现此报文的乘客协议为私网中运行的协议，于是将报文交给该协议处理。



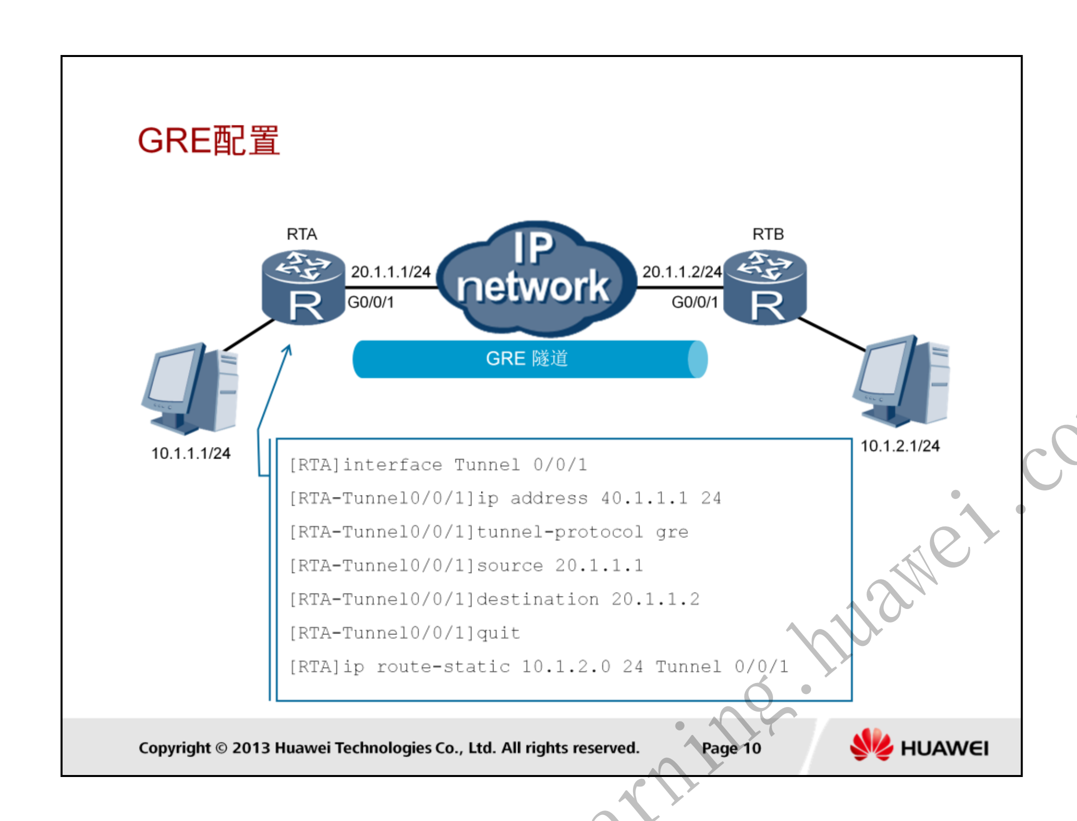
关键字（Key）验证是指对隧道接口进行校验，这种安全机制可以防止错误接收到来自其他设备的报文。关键字字段是一个四字节长的数值，若GRE报文头中的K位为1，则在GRE报文头中会插入关键字字段。只有隧道两端设置的关键字完全一致时才能通过验证，否则报文将被丢弃。



Keepalive检测功能用于在任意时刻检测隧道链路是否处于Keepalive状态，即检测隧道对端是否可达。如果对端不可达，隧道连接就会及时关闭，避免形成数据空洞。使能Keepalive检测功能后，GRE隧道本端会定期向对端发送Keepalive探测报文。若对端可达，则本端会收到对端的回应报文；若对端不可达，则收不到对端的回应报文。如果在隧道一端配置了Keepalive功能，无论对端是否配置Keepalive，配置的Keepalive功能在该端都生效。隧道对端收到Keepalive探测报文，无论是否配置Keepalive，都会给源端发送一个回应报文。

使能Keepalive检测功能后，GRE隧道的源端会创建一个计数器，并周期性地发送Keepalive探测报文，同时进行不可达计数。每发送一个探测报文，不可达计数加1。

如果源端在计数器值达到预先设置的值之前收到回应报文，则表明对端可达。如果计数器值达到预先设置的重试次数，源端还是没有收到回应报文，则认为对端不可达。此时，源端将关闭隧道连接。



interface tunnel *interface-number*命令用来创建Tunnel接口。创建Tunnel接口后，需要配置Tunnel接口的IP地址和Tunnel接口的封装协议。

tunnel-protocol命令用来配置Tunnel接口的隧道协议。

source { *source-ip-address* | *interface-type interface-number* }命令用来配置Tunnel源地址或源接口。

destination *dest-ip-address*命令用来指定Tunnel接口的目的IP地址。

在本端设备和远端设备上还必须存在经过Tunnel转发的路由，这样，需要进行GRE封装的报文才能正确转发。经过Tunnel接口转发的路由可以是静态路由，也可以是动态路由。配置静态路由时，路由的目的地址是GRE封装前原始报文的目的地址，出接口是本端Tunnel接口。

配置验证

```
[RTA]display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2013-08-21 13:37:38
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port, The Maximum Transmit Unit is 1476
Internet Address is 40.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 20.1.1.1 (GigabitEthernet0/0/1), destination 20.1.1.2
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
……
```



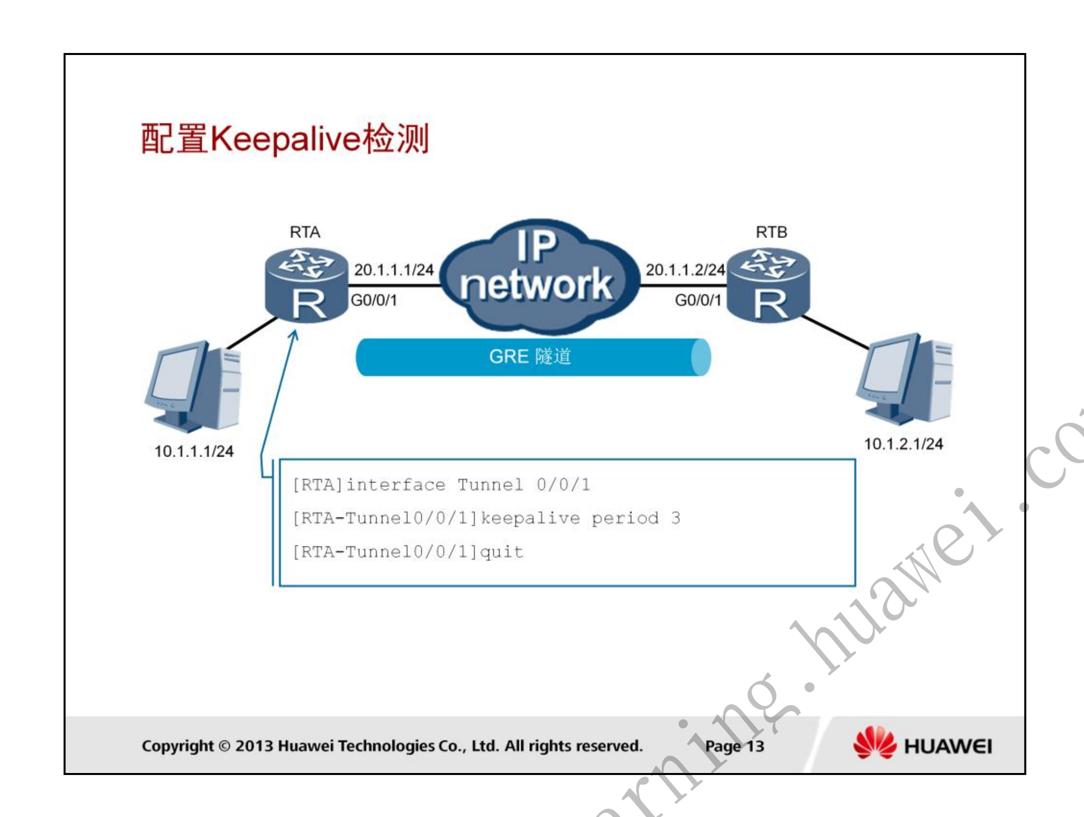

执行**display interface Tunnel 0/0/1**命令，可以查看接口的运行状态和路由信息。如果接口的当前状态和链路层协议的状态均显示为UP，则接口处于正常转发状态。隧道的源地址和目的地址分别为建立GRE隧道使用的物理接口的IP地址。

配置验证

```
[RTA]display ip routing-table
Route Flags: R - relay, D - download to fib
--------------------------------------------------------------
Routing Tables: Public  Destinations : 13       Routes : 14
Destination/Mask Proto  Pre Cost Flags  NextHop   Interface
……
10.1.2.0/24       Static 60   0    RD     40.1.1.2  Tunnel 0/0/1
……
```


Page 12


执行**display ip routing table**命令，可以查看IP路由表，判断GRE隧道连接的两个网络的可达信息。在本示例中，可以看出目的地址为通过GRE隧道可达的网络地址，下一跳地址为GRE隧道远端接口的IP地址。



执行**keepalive** [**period** *period* [**retry-times** *retry-times*]] 命令，可以在GRE隧道接口启用Keepalive检测功能。其中，**period**参数指定Keepalive检测报文的发送周期，默认值为5秒；**retry-times**参数指定Keepalive检测报文的重传次数，默认值为3。如果在指定的重传次数内未收到对端的回应报文，则认为隧道两端通信失败，GRE隧道将被拆除。

配置验证

```
[RTA]display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port, The Maximum Transmit Unit is 1476
Internet Address is 40.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 20.1.1.1 (GigabitEthernet0/0/1), destination 20.1.1.2
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 3 retry-times 3
Checksumming of packets disabled
......
```




执行**display interface tunnel**命令，还可以查看GRE的Keepalive功能是否使能。本示例中，Keepalive检测功能的当前状态显示为启用，且报文的发送周期为3秒，重传次数为3次。



总结

- GRE的应用场景有哪些?
- display interface tunnel命令显示的信息中会包含Internet Address和Tunnel source，这两者的区别是什么?



1. GRE可以解决异种网络的传输问题；GRE隧道扩展了受跳数限制的路由协议的工作范围，支持企业灵活设计网络拓扑；GRE可以与IPSec结合来实现加密传输组播数据。
2. Internet Address代表建立GRE隧道所用的虚拟隧道地址，Tunnel source表示隧道的起点，是设备的出接口物理地址。


谢谢
www.huawei.com

Module-4

优化企业网络的可管理性

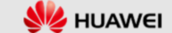

SNMP原理与配置
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

随着网络技术的飞速发展，企业中网络设备的数量成几何级数增长，网络设备的种类也越来越多，这使得企业网络的管理变得十分复杂。

简单网络管理协议SNMP（Simple Network Management Protocol）可以实现对不同种类和不同厂商的网络设备进行统一管理，大大提升了网络管理的效率。



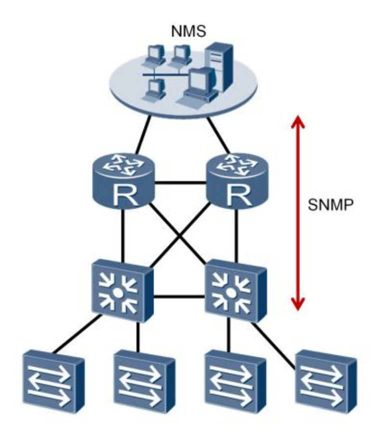


学习目标

学完本课程后，您应该能：

- 掌握SNMP的基本概念
- 掌握SNMP的基本配置

SNMP应用场景



- SNMP用来在网络管理系统NMS和被管理设备之间传输管理信息。

 Page 4



SNMP是广泛应用于TCP/IP网络的一种网络管理协议。SNMP提供了一种通过运行网络管理软件NMS（Network Management System）的网络管理工作站来管理网络设备的方法。

SNMP支持以下几种操作：

1. NMS通过SNMP协议给网络设备发送配置信息。
2. NMS通过SNMP来查询和获取网络中的资源信息。
3. 网络设备主动向NMS上报告警消息，使得网络管理员能够及时处理各种网络问题。

SNMP架构

被管理设备

NMS

SNMP

Agent

Execute

Notify

MIB

- SNMP包括NMS，Agent和MIB等。
- Agent是被管理设备中的一个代理进程。
- MIB是一个数据库，它包含了被管理设备所维护的变量。

 Page 5



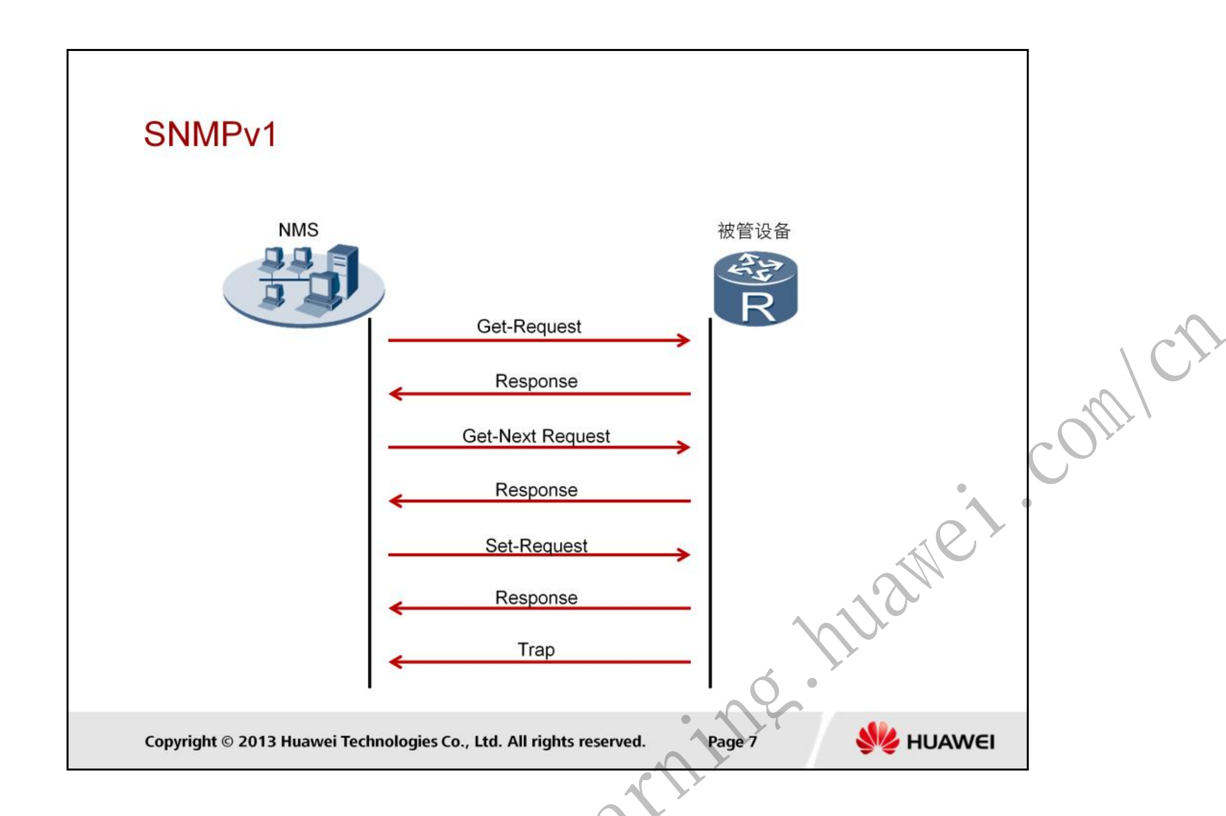
1. NMS是运行在网管主机上的网络管理软件。网络管理员通过操作NMS，向被管理设备发出请求，从而可以监控和配置网络设备。
2. Agent是运行在被管理设备上的代理进程。被管理设备在接收到NMS发出的请求后，由Agent作出响应操作。Agent的主要功能包括：收集设备状态信息、实现NMS对设备的远程操作、向NMS发送告警消息。
3. 管理信息库MIB（Management Information Base）是一个虚拟的数据库，是在被管理设备端维护的设备状态信息集。Agent通过查找MIB来收集设备状态信息。

SNMP版本

版本	描述
SNMPv1	实现方便，安全性弱。
SNMPv2c	有一定的安全性。 现在应用最为广泛。
SNMPv3	定义了一种管理框架，为用户提供了安全的访问机制。

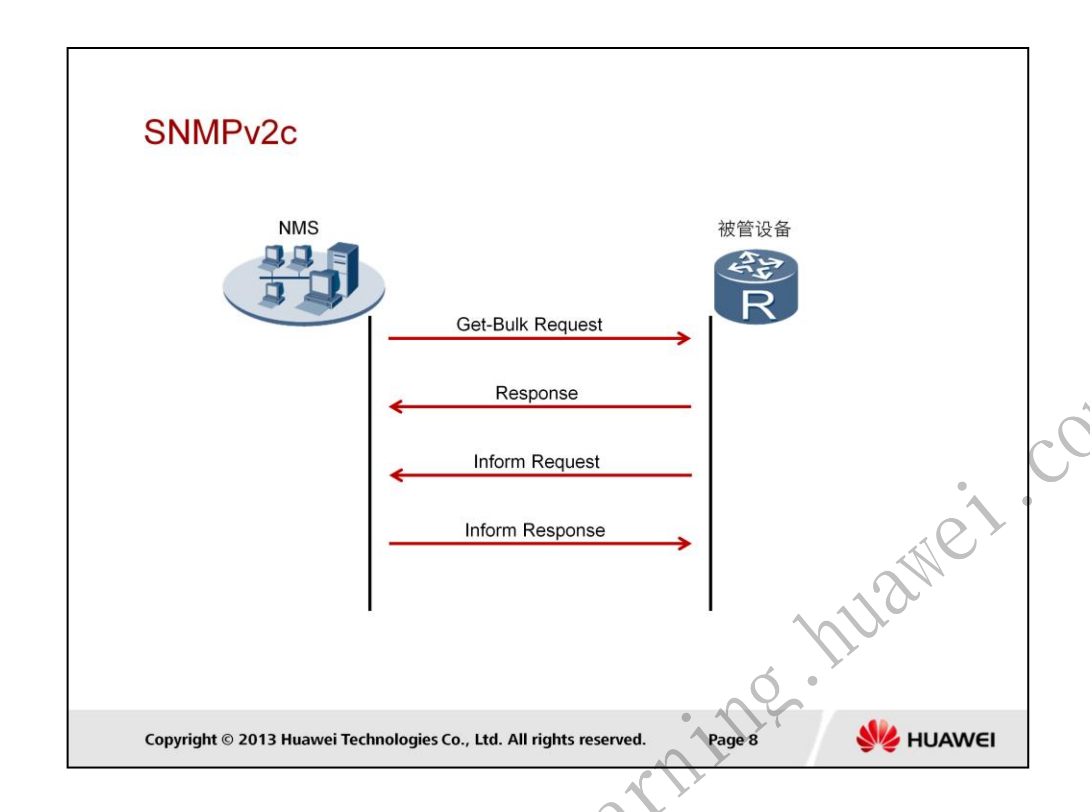


1. SNMPv1：网管端工作站上的NMS与被管理设备上的Agent之间，通过交互SNMPv1报文，可以实现网管端对被管理设备的管理。SNMPv1基本上没有什么安全性可言。
2. SNMPv2c在继承SNMPv1的基础上，其性能、安全性、机密性等方面都有了大的改进。
3. SNMPv3是在SNMPv2基础之上增加、完善了安全和管理机制。SNMPv3体系结构体现了模块化的设计思想，使管理者可以方便灵活地实现功能的增加和修改。SNMPv3的主要特点在于适应性强，可适用于多种操作环境，它不仅可以管理最简单的网络，实现基本的管理功能，也可以提供强大的网络管理功能，满足复杂网络的管理需求。



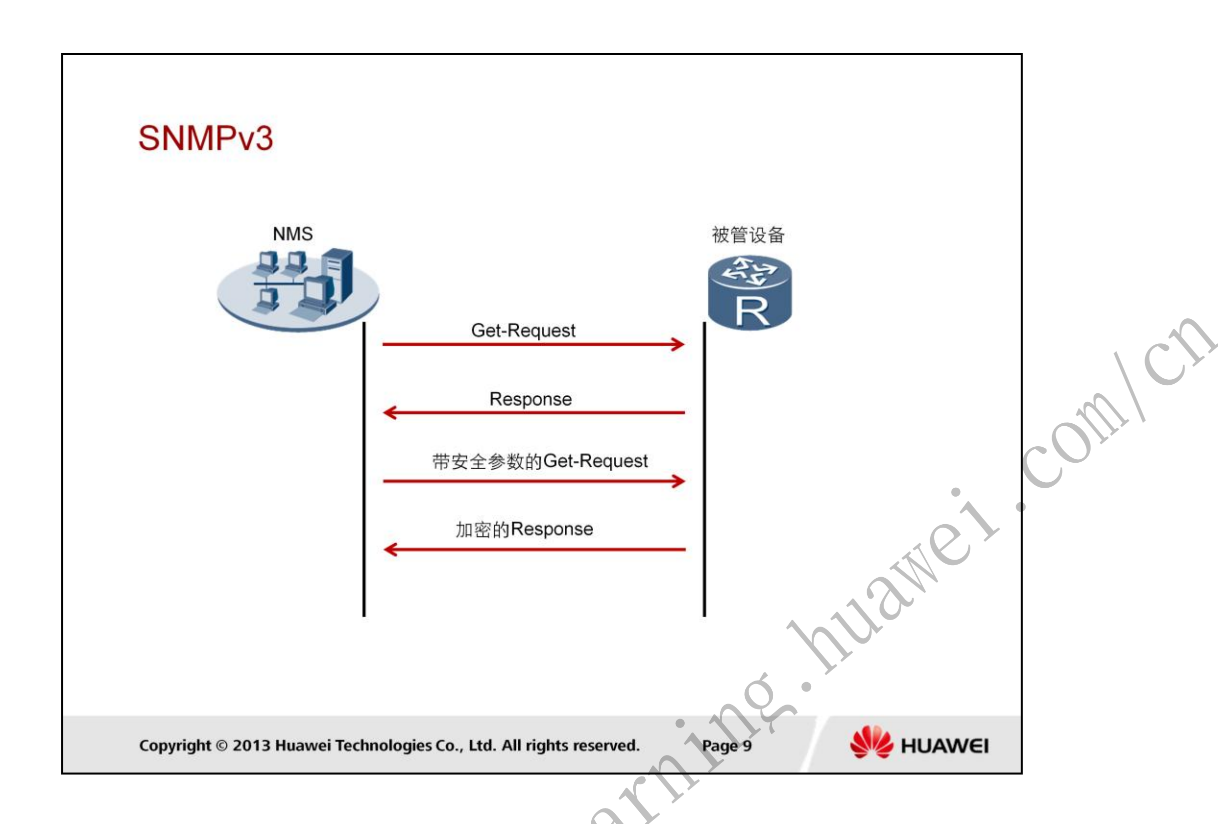
SNMPv1定义了5种协议操作：

1. Get-Request：NMS从代理进程的MIB中提取一个或多个参数值。
2. Get-Next-Request：NMS从代理进程的MIB中按照字典式排序提取下一个参数值。
3. Set-Request：NMS设置代理进程MIB中的一个或多个参数值。
4. Response：代理进程返回一个或多个参数值。它是前三种操作的响应操作。
5. Trap：代理进程主动向NMS发送报文，告知设备上发生的紧急或重要事件。



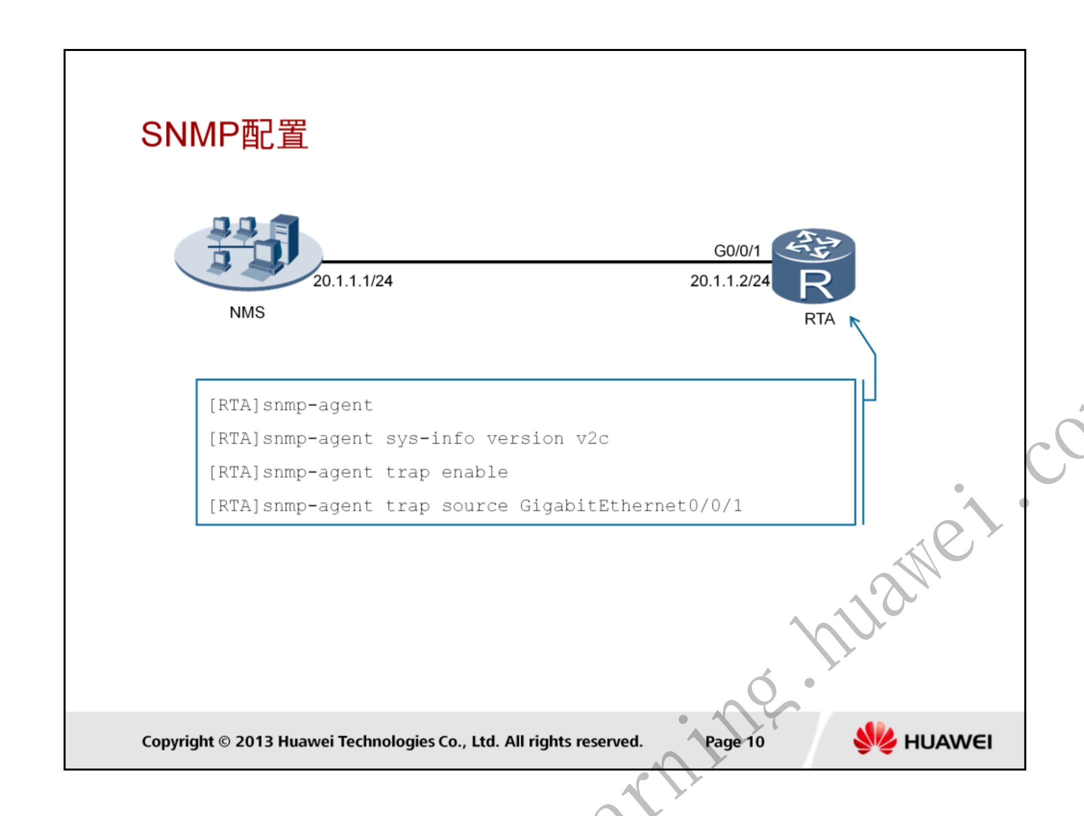
SNMPv2c新增了2种协议操作:

1. GetBulk:相当于连续执行多次GetNext操作。在NMS上可以设置被管理设备在一次GetBulk报文交互时，执行GetNext操作的次数。
2. Inform:被管理设备向NMS主动发送告警。与trap告警不同的是，被管理设备发送Inform告警后，需要NMS进行接收确认。如果被管设备没有收到确认信息则会将告警暂时保存在Inform缓存中，并且会重复发送该告警，直到NMS确认收到了该告警或者发送次数已经达到了最大重传次数。



SNMPv3的实现原理和SNMPv1/SNMPv2c基本一致，主要的区别是SNMPv3增加了身份验证和加密处理。

1. NMS向Agent发送不带安全参数的Get请求报文，向Agent获取安全参数等信息。
2. Agent响应NMS的请求，向NMS反馈所请求的参数。
3. NMS向Agent发送带安全参数的Get请求报文。
4. Agent对NMS发送的请求消息进行认证，认证通过后对消息进行解密，解密成功后，向NMS发送加密的响应。



snmp-agent命令用来使能SNMP代理。

执行**snmp-agent sys-info version [[v1 | v2c | v3] * | all]**命令可以配置SNMP系统信息，其中**version [[v1 | v2c | v3] * | all]**指定设备运行的SNMP版本。缺省情况下，ARG3系列路由器支持SNMPv1，SNMPv2c，SNMPv3版本。

执行**snmp-agent trap enable**命令，可以激活代理向NMS发送告警消息的功能，这一功能激活后，设备将向NMS上报任何异常事件。另外，还需要指定发送告警通告的接口，本示例中指定的是与NMS相连的GigabitEthernet 0/0/1接口。

配置验证

```
[RTA]display snmp-agent sys-info
   The contact person for this managed node:
           R&D Shenzhen, Huawei Technologies Co., Ltd.

   The physical location of this node:
           Shenzhen China

   SNMP version running in the system:
           SNMPv2c
```

 Page 11 HUAWEI

执行**display snmp-agent sys-info**命令，可以查看系统维护的相关信息，包括设备的物理位置和SNMP版本。



总结

- 配置SNMP时，默认的版本号是多少?
- 代理进程Agent发送trap信息给NMS时，目的端口号是多少?



1. 华为ARG3系列路由器默认使能SNMP的所有版本（SNMPv1、SNMPv2c和SNMPv3）。
2. 代理进程使用UDP协议向NMS发送告警消息，目的端口号为162。


谢谢
www.huawei.com


eSight简介
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

随着企业业务的不断发展，企业网络的结构也越来越复杂，并且常常会包含来自不同厂商的多种网络设备。若每种设备都使用与之配套的网管平台来管理，这将给管理员的网络管理工作带来很大不便。

eSight是华为面向企业市场推出的新一代网络运维管理系统，它能够支持多厂商设备的管理，也能支持多种设备的管理，极大地提升了网络管理的效率。





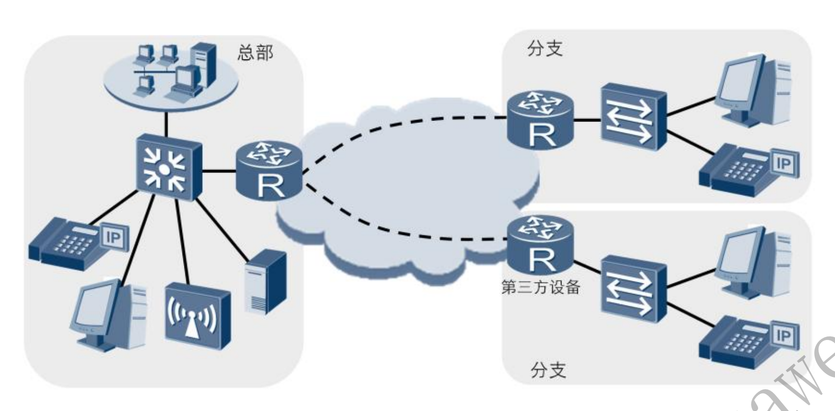
学习目标

学完本课程后，您应该能：

- 了解eSight 在企业网络中的应用场景
- 掌握eSight的常用管理功能



eSight应用场景



- eSight是华为公司推出的新一代面向企业有线/无线园区、企业分支网络、数据中心网络的运维管理系统，能够实现对企业资源、业务、用户的统一管理及智能联动。

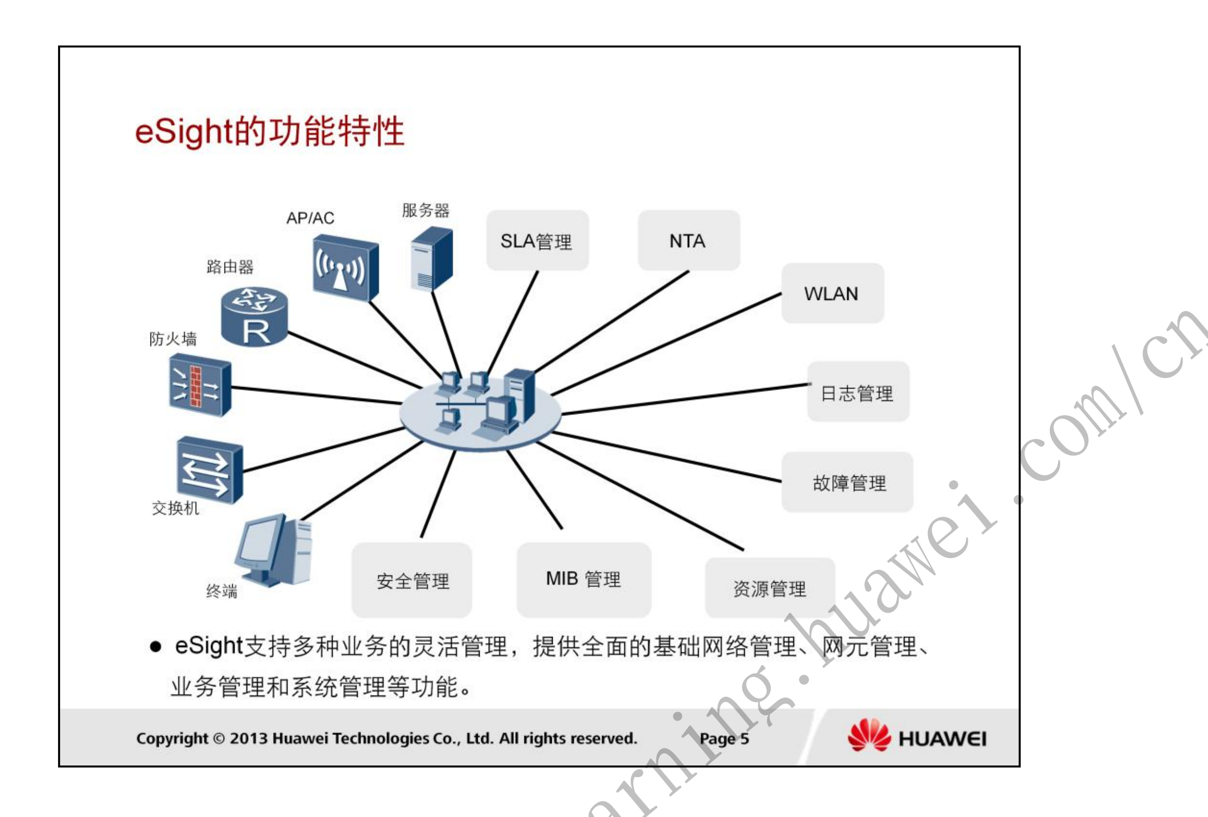
 Page 4



eSight系统是华为公司推出的新一代面向企业有线/无线园区、企业分支网络、数据中心网络的运维管理系统，能够实现对企业资源、业务、用户的统一管理以及智能联动。

eSight支持对多厂商设备进行统一管理，支持对WLAN无线网络进行监控和配置管理，支持对MPLS VPN网络进行监控管理。它可以通过SLA、网络流量分析功能对网络质量进行监视和分析，还可以通过数据中心nCenter组件实现对数据中心虚拟机网络的管理。同时，eSight提供了灵活的开放平台，为企业量身打造自己的智能管理系统提供了基础。

eSight提供了三个版本以适应不同的企业网络规模，这三个版本分别为：精简版、标准版和专业版。精简版支持以下功能：告警管理、性能管理、拓扑管理、配置文件管理、网元管理、链路管理、日志管理、物理资源、电子标签、IP拓扑、智能配置工具、定制设备管理、安全管理、终端接入管理、系统监控工具、数据库备份/恢复工具、故障采集工具和MIB管理。除精简版所支持的功能外，标准版还支持：WLAN管理、网流分析、SLA管理、QoS管理、MPLS VPN管理、MPLS隧道管理、IPSec VPN管理、报表管理、LogCenter、Secure Center和SNMP告警北向接口。除标准版支持的所有功能外，专业版还支持：数据中心nCenter管理、分级网络管理和Linux双机热备。



eSight能够管理多厂商设备，监控、分析并管理网络中的各种服务和网元。例如：

1.SLA组件提供了网络性能度量与诊断功能，用户通过创建SLA任务可以周期性地监控网络的时延、丢包、抖动情况，并根据SLA服务中提供的服务来计算出当前网络的符合度情况。

2.eSight NTA组件提供了一种便捷、经济的网络流量分析方法，能够深入分析网络中的流量数据并提供详细的流量分析报告。

3.WLAN组件提供了有线无线一体化的解决方案，实现了有线网络和无线网络的融合管理。

4.日志管理组件是华为面向行业用户推出的统一日志管理系统，实现对华为安全产品的全面日志分析和安全审计等功能，具有高集成度、高可靠性等特点。

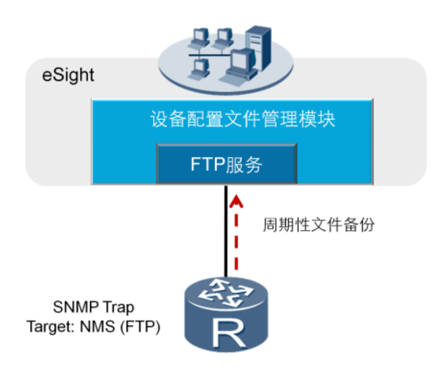
5.故障管理组件可以通过告警实时浏览、告警操作、告警规则设定（屏蔽规则、声音设定）、告警远程通知等手段对网络中的异常情况进行实时监视，便于网络管理员及时采取措施，恢复网络正常运行。

6.资源管理组件可以根据资源在网络中的实际位置将设备划分到不同的子网，对设备进行分组，对同一组中的设备进行批量操作，并允许管理员配置和查询资源信息（包括系统、整机、单板、子卡和端口）。

7.MIB管理组件用于读取、编辑、储存及使用MIB文件。eSight可以通过SNMPv1、SNMPv2c或SNMPv3读取和监控MIB数据。

8.安全管理组件用于管理华为防火墙或统一威胁管理（UTM）环境所布放设备上的大量安全策略。

配置文件管理

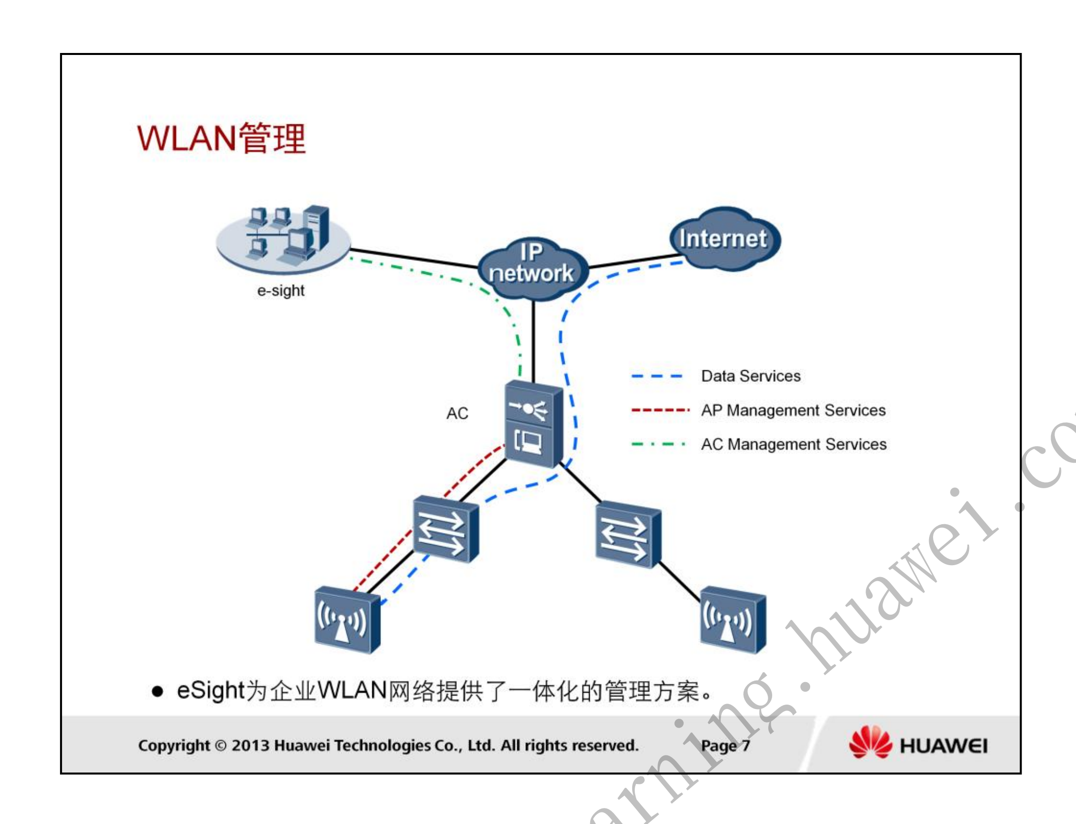


- eSight可以对设备的配置文件进行管理，包括对设备的配置文件进行导入、备份、恢复等操作。

 Page 6 

eSight允许管理员对设备的配置文件执行备份和恢复操作，以确保配置文件的安全性。eSight在配置文件管理操作中作为FTP server，设备作为FTP client。在对设备配置文件进行备份、恢复操作前，需确认文件传输服务FTP参数配置正确，以确保网元与网管之间文件传输服务正常运行。这些参数包括访问FTP服务的用户名和密码、配置文件在eSight上的保存位置，以及FTP服务的类型（FTP、SFTP或TFTP。默认类型为FTP）。

eSight可以指定一个备份任务以定期备份设备的配置文件（每天、每周或每月的某个时间点），也可以配置备份操作的触发条件，如在设备配置发生变更时发送SNMP告警信息，eSight收到告警后执行文件备份操作。



WLAN管理组件为企业网络提供了有线和无线一体化的解决方案，实现了有线网络和无线网络的融合管理。

1.向导式业务批量部署：批量AP统一下发无线业务配置。

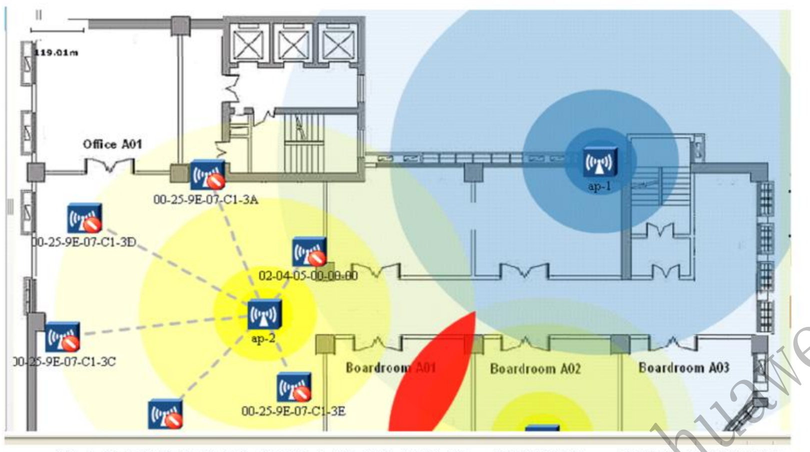
2.无线资源统一管理：AC、AP、无线用户、区域统一管理。

3.用户故障诊断：用户接入网络故障与用户接入后的健康度诊断。

4.无线网络安全检测：WIDS统一监控入侵网络设备与非WIFI干扰源，并提供频谱分析能力。

5.无线网络拓扑可视化管理：实现AC、AP逻辑管理拓扑统一呈现，并基于区域对AP物理布放位置可视化呈现，并展现AP的热图覆盖。

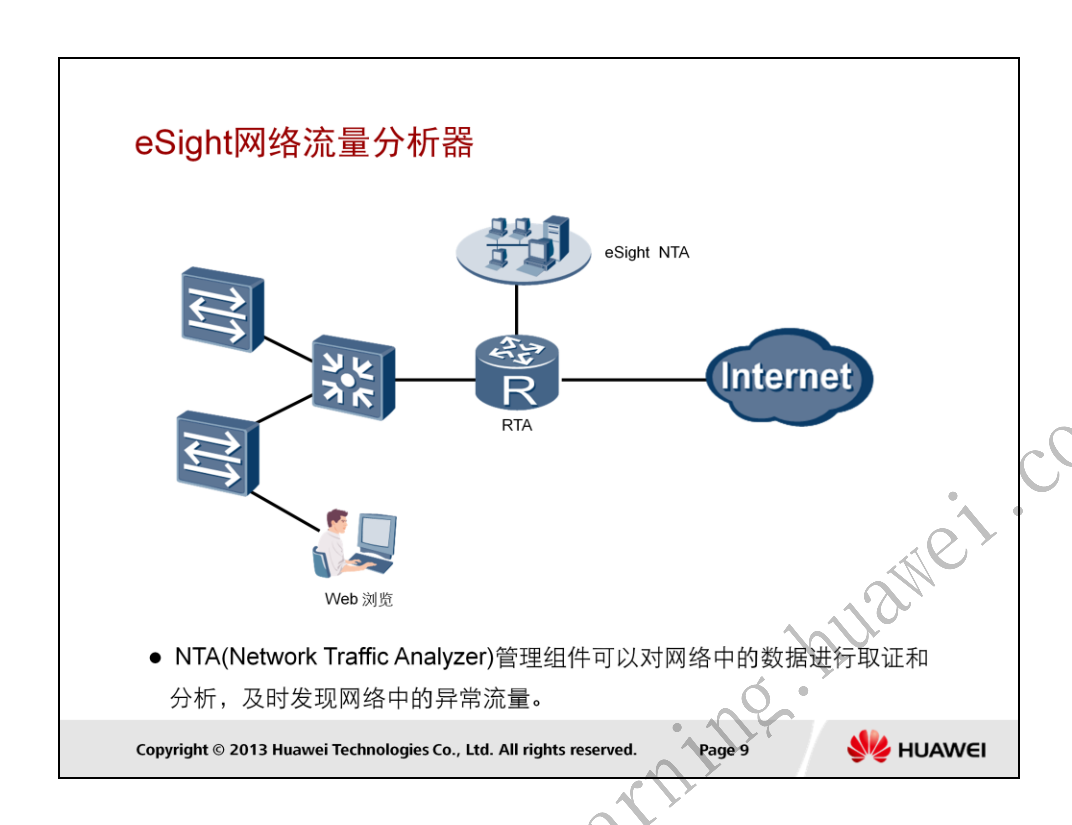
WLAN管理



- eSight可以实现对企业WLAN网络的监控、配置管理、故障诊断等管理功能。

 Page 8 HUAWEI

AP产生的无线射频信号极其容易受到干扰。在设备上启用AP无线射频功能后，用户可以在网管系统中查看AP周围的信号干扰情况。用户还能够根据频谱图确定信道的质量和周围的干扰源。eSight支持五种AP频谱图：实时FFT图、频谱密度图、占空比图、信道质量频谱图和信道质量图。此外，如本例所示，用户还可以在区域内布防AP、查看热点覆盖区域，并及时发现信号覆盖的盲区和冲突区。在启用了无线定位功能的区域中，用户和未授权设备的最新位置会及时更新到拓扑中。这样就可以在位置拓扑中查看热点区域和信号覆盖情况，标注信号冲突的区域、预先布防AP、查看模拟信号覆盖，并检查AP上线后的实际信号覆盖情况。



eSight的NTA组件提供了一种便捷、经济的网络流量分析方法，能够深入分析网络中的流量数据并提供详细的流量分析报告。用户利用NTA能实时监控全网应用流量分布，能及时发现网络中异常流量，并能根据长期的流量分布做好网络规划，做到流量可视、故障可查、规划可依的网络透明化管理。



eSight的NTA组件提供了流量操控板功能，能够实时展示全网流量状态。操控板可显示接口流量排行、接口利用率流量排行、设备流量排行、应用流量排行、主机流量排行、DSCP流量排行和会话流量排行。用户可以自定义流量的显示形式，并可以通过组件生成的流量报表查看流量详情。



eSight支持以饼图、柱状图、曲线图、区域图和图表等各种形式形象地展示流量和各种统计分析数据。统计数据支持以下几种汇总类型：应用汇总、会话汇总、DSCP汇总、源主机汇总、目的主机汇总和接口汇总。eSight可以按照源地址、目的地址和应用等条件过滤流量。eSight能够生成瞬时报表，也可以按照管理员设定的周期定期生成报表。报表生成后，eSight会推送关键信息显示于eSight首页。eSight还能够以邮件方式向用户发送批量下载的详细流量统计信息。



1. eSight网络管理平台有三个版本：精简版、标准版和专业版。


谢谢
www.huawei.com

Module-5

迁移企业网络至IPv6


IPv6基础介绍
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

随着Internet规模的扩大，IPv4地址空间已经消耗殆尽。针对IPv4的地址短缺问题，曾先后出现过CIDR和NAT等临时性解决方案，但是CIDR和NAT都有各自的弊端，并不能作为IPv4地址短缺问题的彻底解决方案。另外，安全性、QoS(服务质量)、简便配置等要求也表明需要一个新的协议来根本解决目前IPv4面临的问题。

IETF在20世纪90年代提出了下一代互联网协议 – IPv6，IPv6支持几乎无限的地址空间。IPv6使用了全新的地址配置方式，使得配置更加简单。IPv6还采用了全新的报文格式，提高了报文处理的效率、安全性，也能更好的支持QoS。





学习目标

学完本课程后，您应该能：

- 掌握IPv6的基本概念
- 掌握IPv6地址格式和地址类型
- 掌握IPv6无状态地址配置的过程

IPv6地址

版本	长度	地址数量
IPv4	32 bit	4,294,967,296
IPv6	128 bit	340,282,366,920,938,463,374,607,431,768,211,456

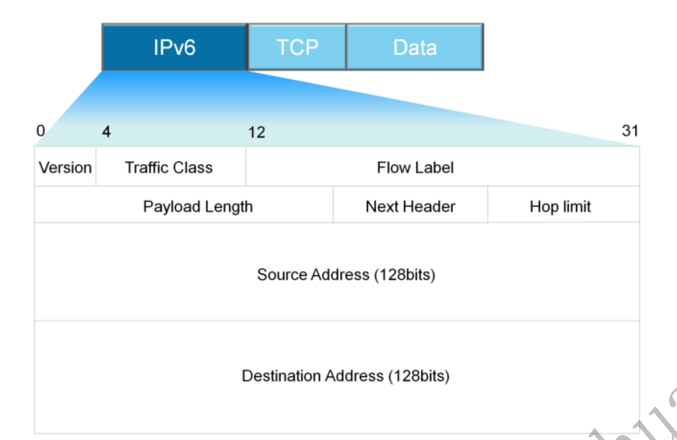
- IPv4地址空间已经消耗殆尽，近乎无限的地址空间是IPv6的最大优势。



在因特网发展初期，IPv4以其协议简单、易于实现、互操作性好的优势而得到快速发展。然而，随着因特网的迅猛发展，IPv4地址不足等设计缺陷也日益明显。IPv4理论上仅仅能够提供的地址数量是43亿，但是由于地址分配机制等原因，实际可使用的数量还远远达不到43亿。因特网的迅猛发展令人始料未及，同时也带来了地址短缺的问题。针对这一问题，曾先后出现过几种解决方案，比如CIDR和NAT。但是CIDR和NAT都有各自的弊端和不能解决的问题，在这样的情况下，IPv6的应用和推广便显得越来越急迫。

IPv6是Internet工程任务组（IETF）设计的一套规范，它是网络层协议的第二代标准协议，也是IPv4（Internet Protocol Version 4）的升级版本。IPv6与IPv4的最显著区别是，IPv4地址采用32比特标识，而IPv6地址采用128比特标识。128比特的IPv6地址可以划分更多地址层级、拥有更广阔的地址分配空间，并支持地址自动配置。

IPv6基本报头



- IPv6的基本报头在IPv4报头的基础上，增加了流标签域，去除了一些冗余字段，使报文头的处理更为简单、高效。

 Page 5



IPv6报文由IPv6基本报头、IPv6扩展报头以及上层协议数据单元三部分组成。

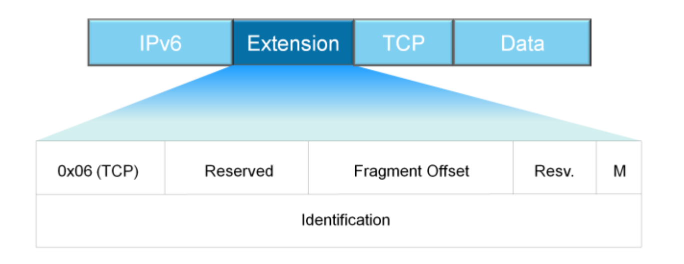
基本报头中的各字段解释如下：

1. Version：版本号，长度为4bit。对于IPv6，该值为6。
2. Traffic Class：流类别，长度为8bit，它等同于IPv4报头中的TOS字段，表示IPv6数据报的类或优先级，主要应用于QoS。
3. Flow Label：流标签，长度为20bit，它用于区分实时流量。流可以理解为特定应用或进程的来自某一源地址发往一个或多个目的地址的连续单播、组播或任播报文。IPv6中的流标签字段、源地址字段和目的地址字段一起为特定数据流指定了网络中的转发路径。这样，报文在IP网络中传输时会保持原有的顺序，提高了处理效率。随着三网合一的发展趋势，IP网络不仅要求能够传输传统的数据报文，还需要能够传输语音、视频等报文。这种情况下，流标签字段的作用就显得更加重要。
4. Payload Length：有效载荷长度，长度为16bit，它是指紧跟IPv6报头的数据报的其它部分。
5. Next Header：下一个报头，长度为8bit。该字段定义了紧跟在IPv6报头后面的第一个扩展报头（如果存在）的类型。
6. 跳数限制（Hop Limit），长度为8bit，该字段类似于IPv4报头中的Time to Live字段，它定义了IP数据报所能经过的最大跳数。每经过一个路由器，该数值减去1；当该字段的值为0时，数据报将被丢弃。

7. Source Address：源地址，长度为128bit，表示发送方的地址。
8. Destination Address：目的地址，长度为128bit，表示接收方的地址。

与IPv4相比，IPv6报头去除了IHL、Identifier、Flags、Fragment Offset、Header Checksum、 Options、Padding域，只增了流标签域，因此IPv6报文头的处理较IPv4大大简化，提高了处理效率。另外，IPv6为了更好支持各种选项处理，提出了扩展头的概念。

IPv6扩展报头



- IPv6扩展报头是跟在IPv6基本报头后面的可选报头，可以有一个或多个。
- 如图所示的扩展报头是分片扩展报头。

 Page 7



IPv6增加了扩展报头，使得IPv6报头更加简化。一个IPv6报文可以包含0个、1个或多个扩展报头，仅当需要路由器或目的节点做某些特殊处理时，才由发送方添加一个或多个扩展报头。IPv6支持多个扩展报头，各扩展报头中都含有一个下一个报头字段，用于指明下一个扩展报头的类型。这些报头必须按照以下顺序出现：

1. IPv6基本报头
2. 逐跳选项扩展报头
3. 目的选项扩展报头
4. 路由扩展报头
5. 分片扩展报头
6. 认证扩展报头
7. 封装安全有效载荷扩展报头
8. 目的选项扩展报头（指那些将被分组报文的最终目的地处理的选项）
9. 上层协议数据报文

除了目的选项扩展报头外，每个扩展报头在一个报文中最多只能出现一次。目的选项扩展报头在一个报文中最多也只能出现两次，一次是在路由扩展报头之前，另一次是在上层协议扩展报头之前。

IPv6地址格式

2001:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

0010 0000 0000 0001

128bits

2001:0DB8:0000:0000:0000:0000:0346:8D58

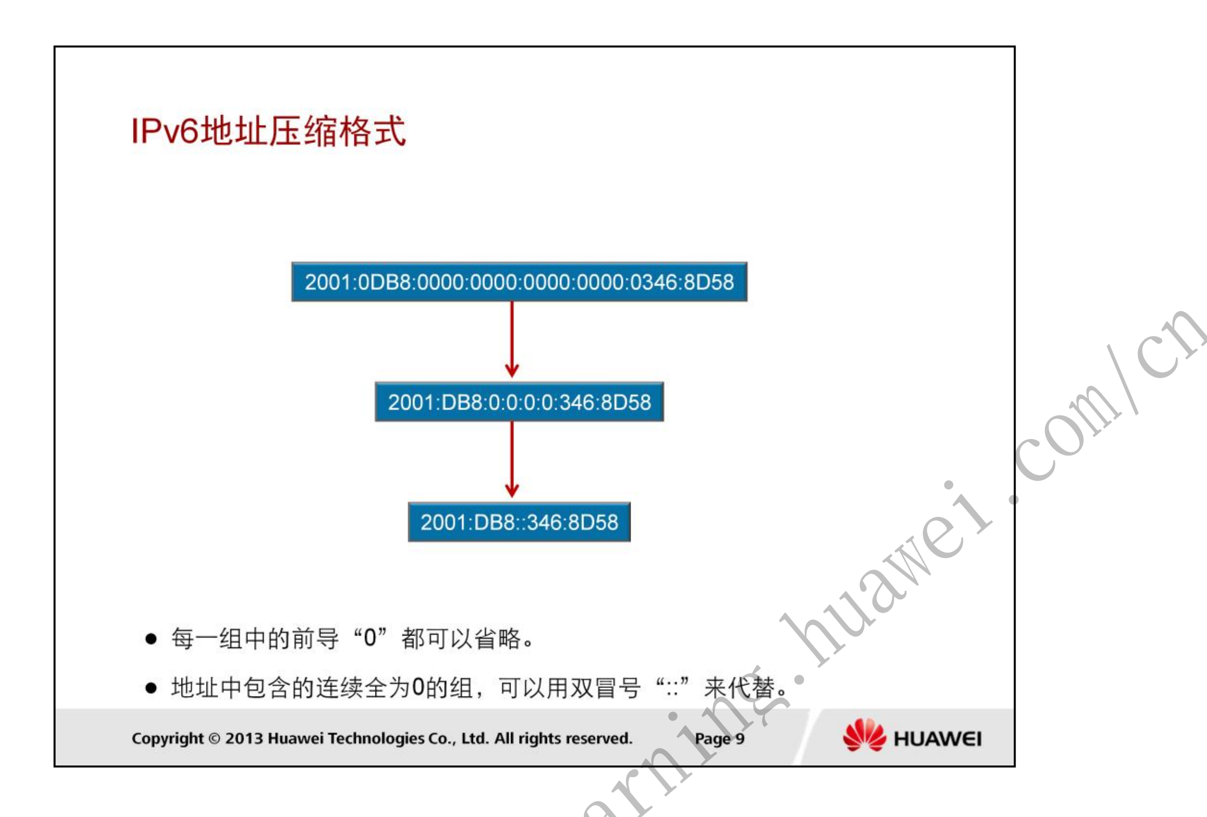
IPv6 前缀　　接口标识

- IPv6地址长度为128比特，每16比特划分为一段，每段由4个十六进制数表示，并用冒号隔开。
- IPv6地址包括网络前缀和接口标识两部分。

 Page 8



IPv6地址长度为128比特，用于标识一个或一组接口。IPv6地址通常写作xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx，其中xxxx是4个十六进制数，等同于一个16比特二进制数；八组xxxx共同组成了一个128比特的IPv6地址。一个IPv6地址由IPv6地址前缀和接口ID组成，IPv6地址前缀用来标识IPv6网络，接口ID用来标识接口。



由于IPv6地址长度为128比特，书写时会非常不方便。此外，IPv6地址的巨大地址空间使得地址中往往会包含多个0。为了应对这种情况，IPv6提供了压缩方式来简化地址的书写。压缩规则如下：

1. 每16比特组中的前导0可以省略。
2. 地址中包含的连续两个或多个均为0的组，可以用双冒号“::”来代替。需要注意的是，在一个IPv6地址中只能使用一次双冒号“::”，否则，设备将压缩后的地址恢复成128位时，无法确定每段中0的个数。

本示例展示了如何利用压缩规则对IPv6地址进行简化表示。

IPv6地址分类

地址范围	描述
2000::/3	全球单播地址
2001:0DB8::/32	保留地址
FE80::/10	链路本地地址
FF00::/8	组播地址
::/128	未指定地址
::1/128	环回地址

- IPv6地址分为单播地址、任播地址、组播地址三种类型。

 Page 10



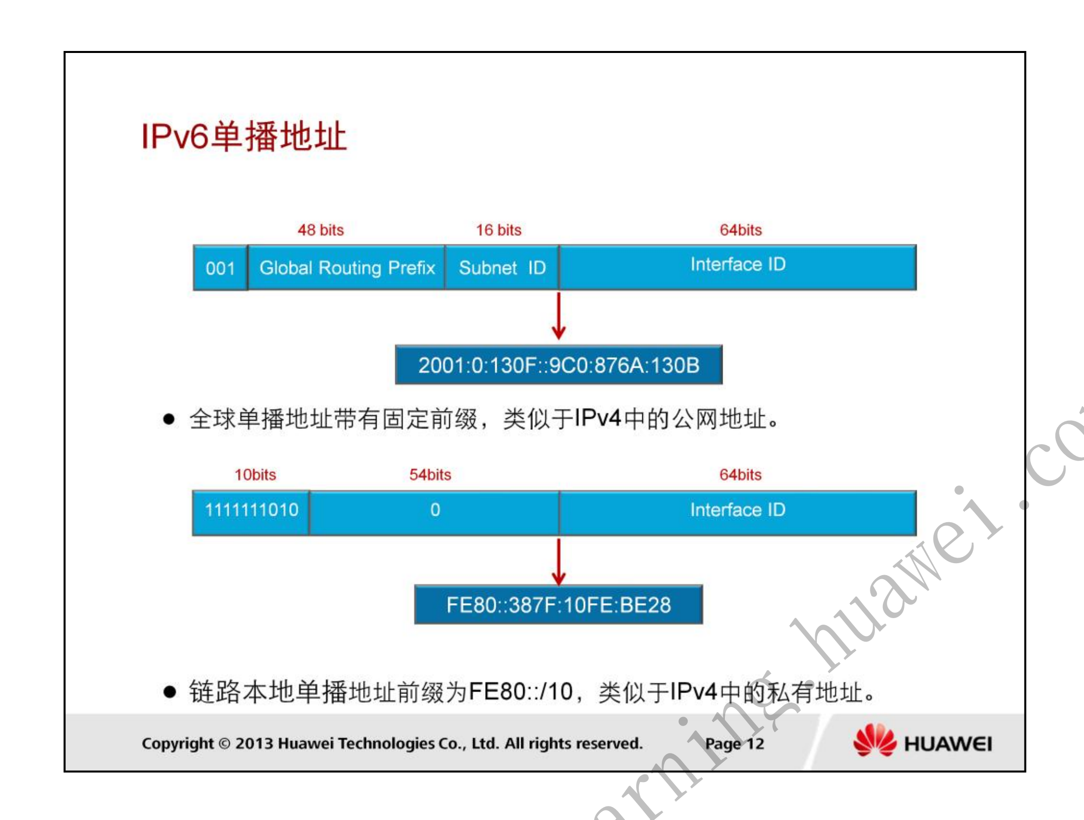
目前，IPv6地址空间中还有很多地址尚未分配。这一方面是因为IPv6有着巨大的地址空间，足够在未来很多年使用，另一方面是因为寻址方案还有待发展，同时关于地址类型的适用范围也多有值得商榷的地方。

目前，有一小部分全球单播地址已经由IANA（互联网名称与数字地址分配机构ICANN的一个分支）分配给了用户。单播地址的格式是2000::/3，代表公共IP网络上任意可及的地址。IANA负责将该段地址范围内的地址分配给多个区域互联网注册管理机构（RIR）。RIR负责全球5个区域的地址分配。以下几个地址范围已经分配：2400::/12 (APNIC)、2600::/12 (ARIN)、2800::/12 (LACNIC)、2A00::/12 (RIPE NCC)和2C00::/12 (AfriNIC)，它们使用单一地址前缀标识特定区域中的所有地址。2000::/3地址范围中还为文档示例预留了地址空间，例如2001:0DB8::/32。

链路本地地址只能在连接到同一本地链路的节点之间使用。可以在自动地址分配、邻居发现和链路上没有路由器的情况下使用链路本地地址。以链路本地地址为源地址或目的地址的IPv6报文不会被路由器转发到其他链路。链路本地地址的前缀是FE80::/10。

组播地址的前缀是FF00::/8。组播地址范围内的大部分地址都是为特定组播组保留的。跟IPv4一样，IPv6组播地址还支持路由协议。IPv6中没有广播地址。组播地址替代广播地址可以确保报文只发送给特定的组播组而不是IPv6网络中的任意终端。

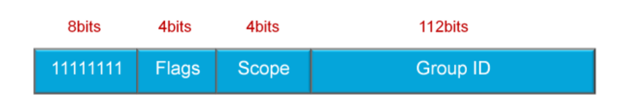
IPv6还包括一些特殊地址，比如未指定地址::/128。如果没有给一个接口分配IP地址，该接口的地址则为::/128。需要注意的是，不能将未指定地址跟默认IP地址::/0相混淆。默认IP地址::/0跟IPv4中的默认地址0.0.0.0/0类似。环回地址127.0.0.1在IPv6中被定义为保留地址::1/128。



单播地址主要包含全球单播地址和链路本地地址。全球单播地址（例如2000::/3）带有固定的地址前缀，即前三位为固定值001。其地址结构是一个三层结构，依次为全球路由前缀、子网标识和接口标识。全球路由前缀由RIR和互联网服务供应商（ISP）组成，RIR为ISP分配IP地址前缀。子网标识定义了网络的管理子网。

链路本地单播地址的前缀为FE80::/10，表示地址最高10位值为1111111010。前缀后面紧跟的64位是接口标识，这64位已足够主机接口使用，因而链路本地单播地址的剩余54位为0。本示例展示了上述两种单播地址类型。

IPv6组播地址



地址范围	描述
FF02::1	链路本地范围所有节点
FF02::2	链路本地范围所有路由器

- 所有IPv6组播地址都以FF开始。
- IPv6为需要使用组播发送数据的协议预留了一些组播组。

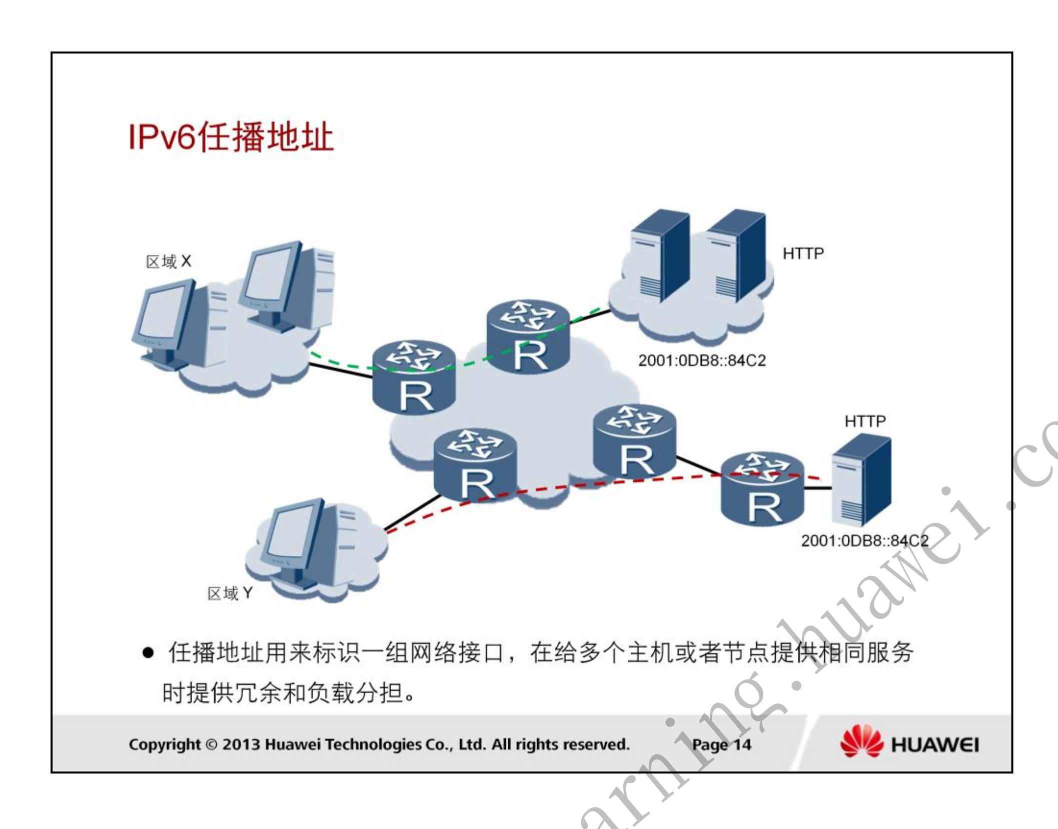
 Page 13



IPv6的组播与IPv4相同，用来标识一组接口，一般这些接口属于不同的节点。一个节点可能属于0到多个组播组。目的地址为组播地址的报文会被该组播地址标识的所有接口接收。

一个IPv6组播地址是由前缀、标志（Flag）字段、范围（Scope）字段以及组播组ID（Group ID）4个部分组成：

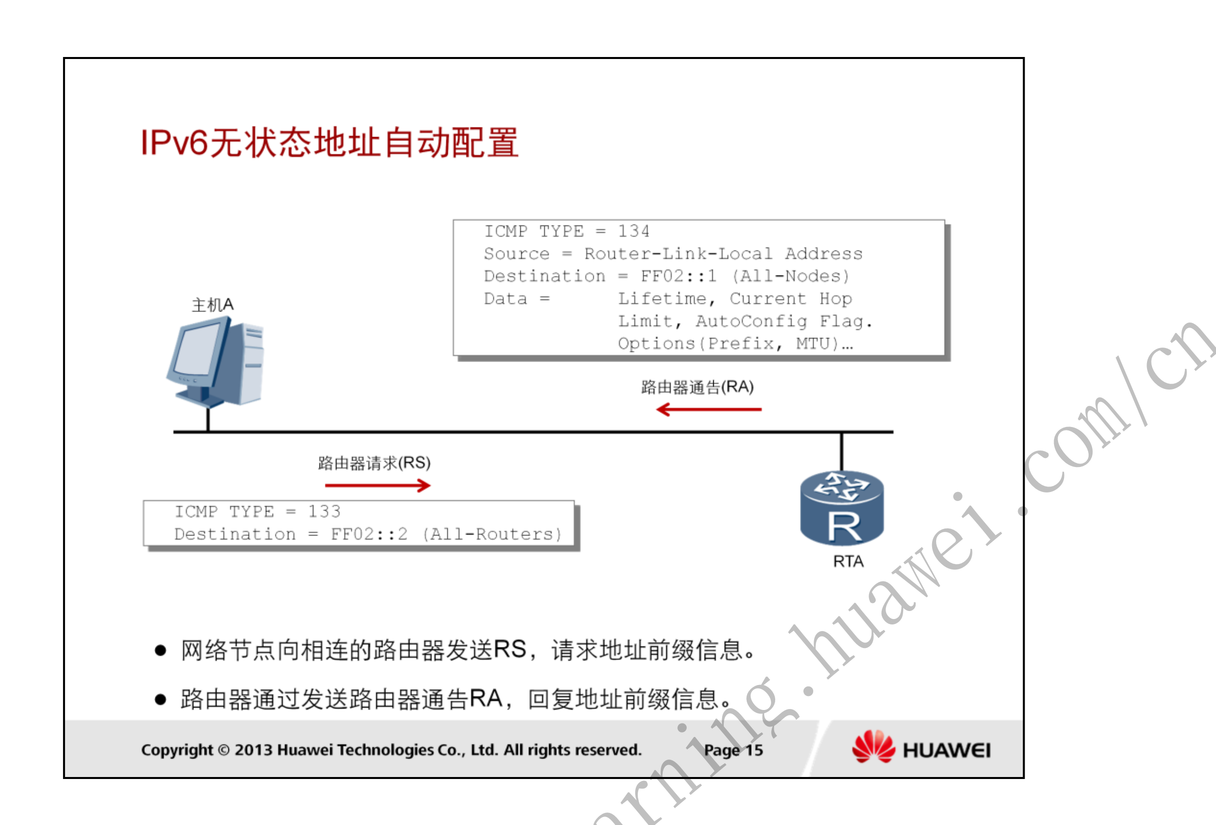
1. 前缀：IPv6组播地址的前缀是FF00::/8（1111 1111）。
2. 标志字段（Flag）：长度4bit，目前只使用了最后一个比特（前三位必须置0），当该位值为0时，表示当前的组播地址是由IANA所分配的一个永久分配地址；当该值为1时，表示当前的组播地址是一个临时组播地址（非永久分配地址）。
3. 范围字段（Scope）：长度4bit，用来限制组播数据流在网络中发送的范围。
4. 组播组ID（Group ID）：长度112bit，用以标识组播组。目前，RFC2373并没有将所有的112位都定义成组标识，而是建议仅使用该112位的最低32位作为组播组ID，将剩余的80位都置0，这样，每个组播组ID都可以映射到一个唯一的以太网组播MAC地址（RFC2464）。



任播地址标识一组网络接口（通常属于不同的节点）。目标地址是任播地址的数据包将发送给其中路由意义上最近的一个网络接口。任播过程涉及一个任播报文发起方和一个或多个响应方。任播报文的发起方通常为请求某一服务（DNS查找）的主机或请求返还特定数据（例如，HTTP网页信息）的主机。任播地址与单播地址在格式上无任何差异，唯一的区别是一台设备可以给多台具有相同地址的设备发送报文。

企业网络中运用任播地址有很多优势。其中一个优势是业务冗余。比如，用户可以通过多台使用相同地址的服务器获取同一个服务（例如，HTTP）。这些服务器都是任播报文的响应方。如果不是采用任播地址通信，当其中一台服务器发生故障时，用户需要获取另一台服务器的地址才能重新建立通信。如果采用的是任播地址，当一台服务器发生故障时，任播报文的发起方能够自动与使用相同地址的另一台服务器通信，从而实现业务冗余。

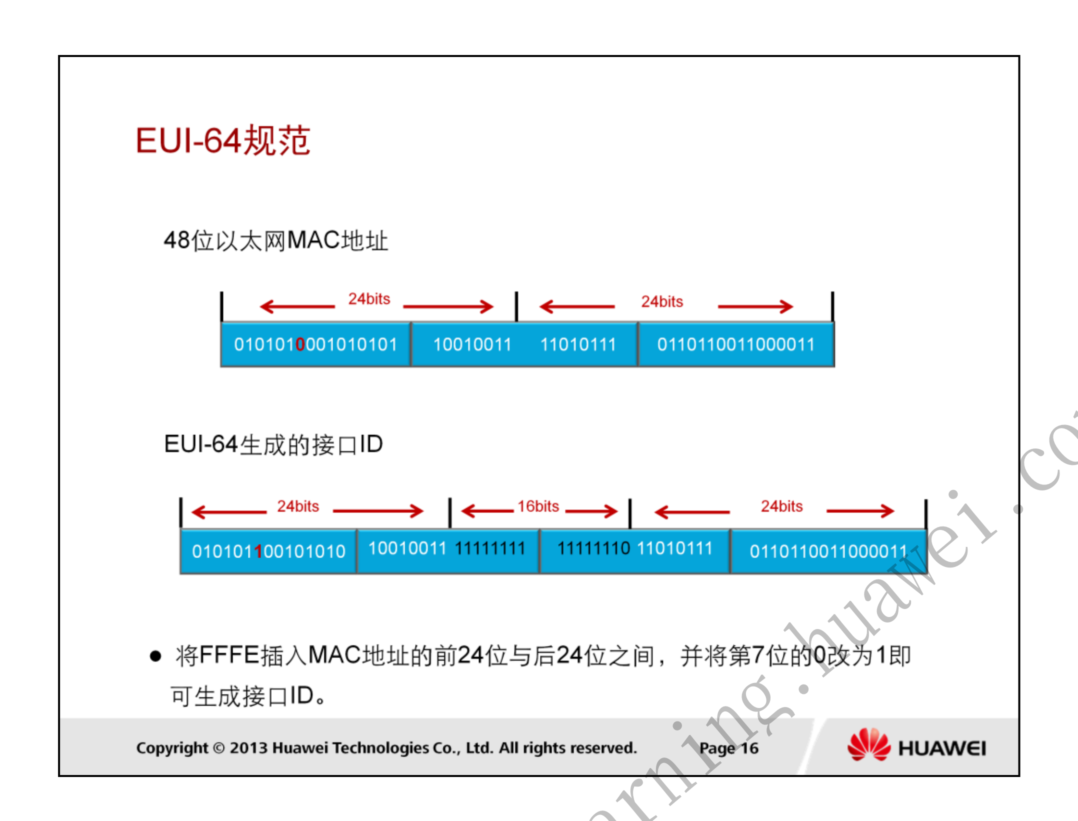
使用多服务器接入还能够提高工作效率。例如，用户（即任播地址的发起方）浏览公司网页时，与相同的单播地址建立一条连接，连接的对端是具有相同任播地址的多个服务器。用户可以从不同的镜像服务器分别下载html文件和图片。用户利用多个服务器的带宽同时下载网页文件，其效率远远高于使用单播地址进行下载。



IPv6支持无状态地址自动配置，无需使用诸如DHCP之类的辅助协议，主机即可获取IPv6前缀并自动生成接口ID。路由器发现功能是IPv6地址自动配置功能的基础，主要通过以下两种报文实现：

RA报文：每台路由器为了让二层网络上的主机和其它路由器知道自己的存在，定期以组播方式发送携带网络配置参数的RA报文。RA报文的Type字段值为134。

RS报文：主机接入网络后可以主动发送RS报文。RA报文是由路由器定期发送的，但是如果主机希望能够尽快收到RA报文，它可以立刻主动发送RS报文给路由器。网络上的路由器收到该RS报文后会立即向相应的主机单播回应RA报文，告知主机该网段的默认路由器和相关配置参数。RS报文的Type字段值为133。



为了通过IPv6网络进行通信，各接口必须获取有效的IPv6地址，以下三种方式可以用来配置IPv6地址的接口ID：网络管理员手动配置；通过系统软件生成；采用扩展唯一标识符（EUI-64）格式生成。就实用性而言，EUI-64格式是IPv6生成接口ID的最常用方式。IEEE EUI-64标准采用接口的MAC地址生成IPv6接口ID。MAC地址只有48位，而接口ID却要求64位。MAC地址的前24位代表厂商ID，后24位代表制造商分配的唯一扩展标识。MAC地址的第七高位是一个U/L位，值为1时表示MAC地址全局唯一，值为0时表示MAC地址本地唯一。在MAC地址向EUI-64格式的转换过程中，在MAC地址的前24位和后24位之间插入了16比特的FFFE，并将U/L位的值从0变成了1，这样就生成了一个64比特的接口ID，且接口ID的值全局唯一。接口ID和接口前缀一起组成接口地址。

IPv6无状态地址DAD检查

```
ICMP TYPE = 135
Source = ::
Destination = FF02::1:FF00:1
Data = 2000::1
Query = Is this address in use?
```

主机A

2000::1

试验地址

邻居请求(NS)

R

邻居通告(NA)

主机B

2000::1

```
ICMP TYPE = 136
Source = 2000::1
Destination = FF02::1
Data = 2000::1
Reply = I am using this address.
```

- 当为接口配置IPv6地址时，DAD用来在本地链路范围内检测将要使用的IPv6地址是否唯一。

 Page 17 HUAWEI

设备在给接口分配IPv6单播地址之前会进行重复地址检测（DAD），确认是否有其它的节点使用了该地址。尤其是在地址自动配置的时候，进行DAD检测是很必要的。一个IPv6单播地址在分配给一个接口之后且通过重复地址检测之前称为试验地址，此时该接口不能使用这个试验地址进行单播通信，但是仍然会加入两个组播组：ALL-nodes组播组和Solicited-node组播组。Solicited-node组播组由单播或任播地址的后24位加上地址前缀FF02:0:0:0:0:1:FF00::/104组成。例如，本示例中配置的试验地址为2000::1，该地址被加入Solicited-node组播组FF02::1:FF00:1。

IPv6重复地址检测技术和IPv4中的免费ARP类似：用于地址分配或主机连接网络时检测重复的IPv4主机地址。节点向一个自己将使用的试验地址所在的Solicited-node组播组发送一个以该试验地址为请求的目标地址的邻居请求（NS）报文，如果收到某个其它站点回应的邻居通告（NA）报文，就证明该地址已被网络上使用，节点将不能使用该试验地址进行通信。这种情况下，网络管理员需要手动为该节点分配另外一个地址。



总结

- 2001:0DB8:0000:0000:0000:0000:032A:2D70，此IPv6地址压缩到最短是多少?
- IPv6主机无状态地址自动配置的过程是什么?

 Page 18



1. 地址2001:0DB8:0000:0000:0000:0000:032A:2D70可压缩为2001:DB8::32A:2D70。鉴于IPv6近乎无限的地址空间，两个或多个均为0的组可以用双冒号来显示，但是双冒号只能用一次。每组中的前导0都可以省略，但是最后一个0不可以省略。
2. IPv6主机首先通过路由器发现功能来获取地址前缀信息，之后通过向接口已有的48比特MAC地址中插入16比特的FFEE生成接口ID，在生成了IPv6地址后会通过重复地址检测来确认地址是否唯一。


谢谢
www.huawei.com


IPv6路由基础
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

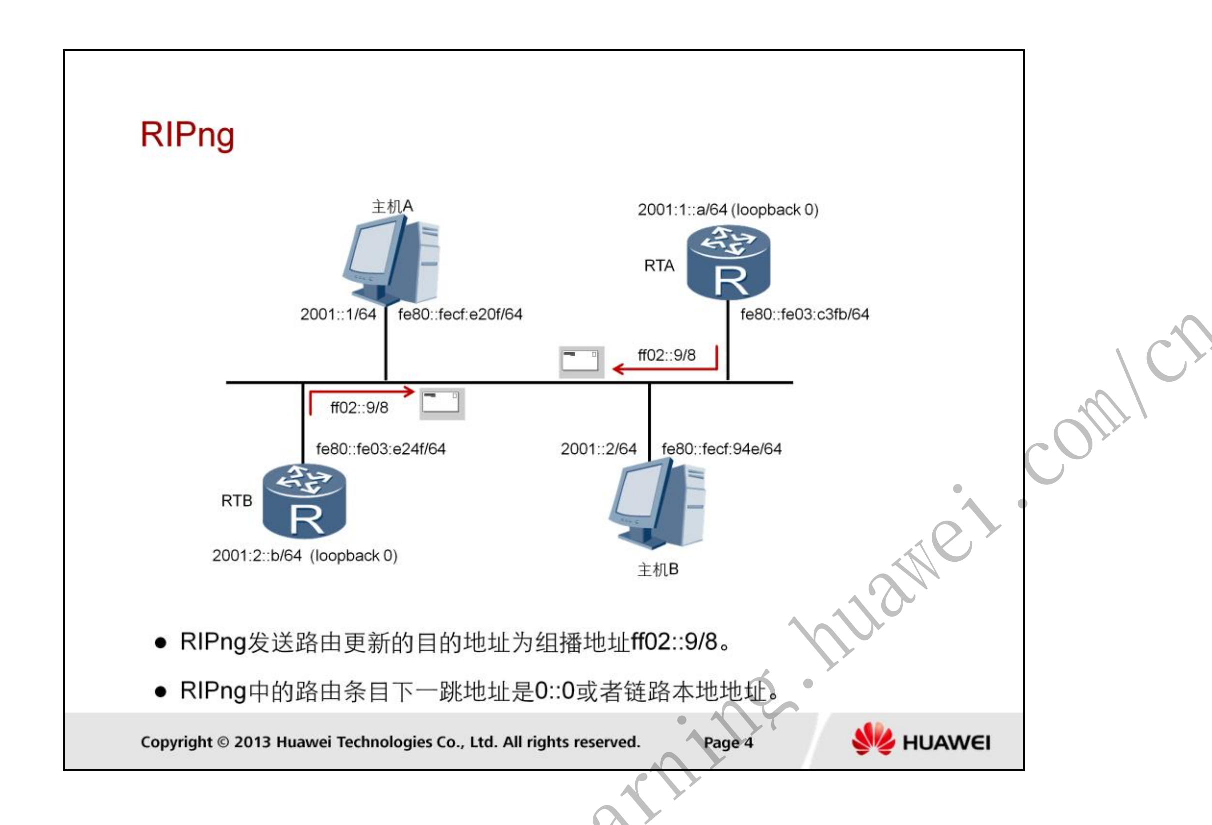
在企业网络中，IPv6技术的应用越来越普及。IETF组织针对IPv6网络制定了两种路由协议RIPng和OSPFv3。



学习目标

学完本课程后，您应该能：

- 掌握RIPng和OSPFv3的工作原理
- 掌握RIPng和OSPFv3的配置



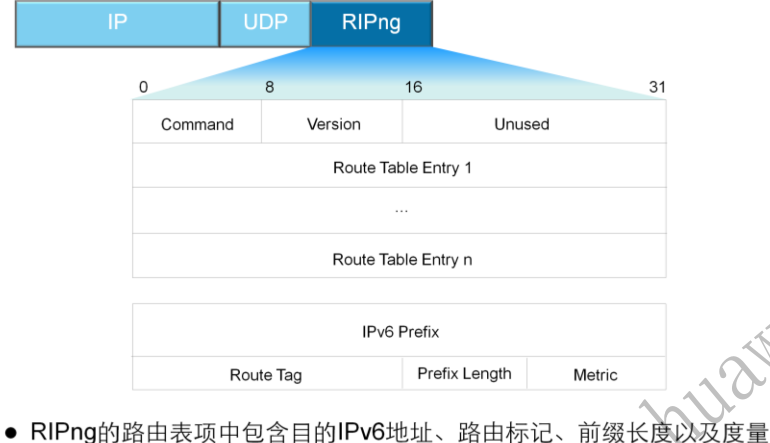
RIPng是为IPv6网络设计的下一代距离矢量路由协议。与早期的IPv4版本的RIP类似，RIPng同样遵循距离矢量原则。RIPng保留了RIP的多个主要特性，比如，RIPng规定每一跳的开销度量值也为1，最大跳数也为15。

RIPng与RIP的最主要区别在于，RIPng使用了IPv6组播地址ff02::9作为目的地址来传送路由更新报文，而RIPv2使用的是组播地址224.0.0.9。

IPv4路由协议一般采用公网地址或私网地址作为路由条目的下一跳地址，而IPv6路由协议通常采用链路本地地址作为路由条目的下一跳地址。

本示例中的两台路由器位于同一个广播网段，RTA和RTB的loopback 0接口使用的是全球单播地址。然而，RTA和RTB的物理接口在使用RIPng传送路由信息时，路由条目的下一跳地址只能是链路本地地址。例如，如果RTA收到的路由条目的下一跳地址为fe80::fe03:e24f，RTA就会认为目的地址为2001::b的网络可达。需要注意的是，如果采用的是EUI-64格式生成的接口链路本地地址，替换接口板后，链路本地地址也会随着发生变化。为了避免这种情况，可以手动配置链路本地地址。

RIPng报文格式



- RIPng的路由表项中包含目的IPv6地址、路由标记、前缀长度以及度量值。

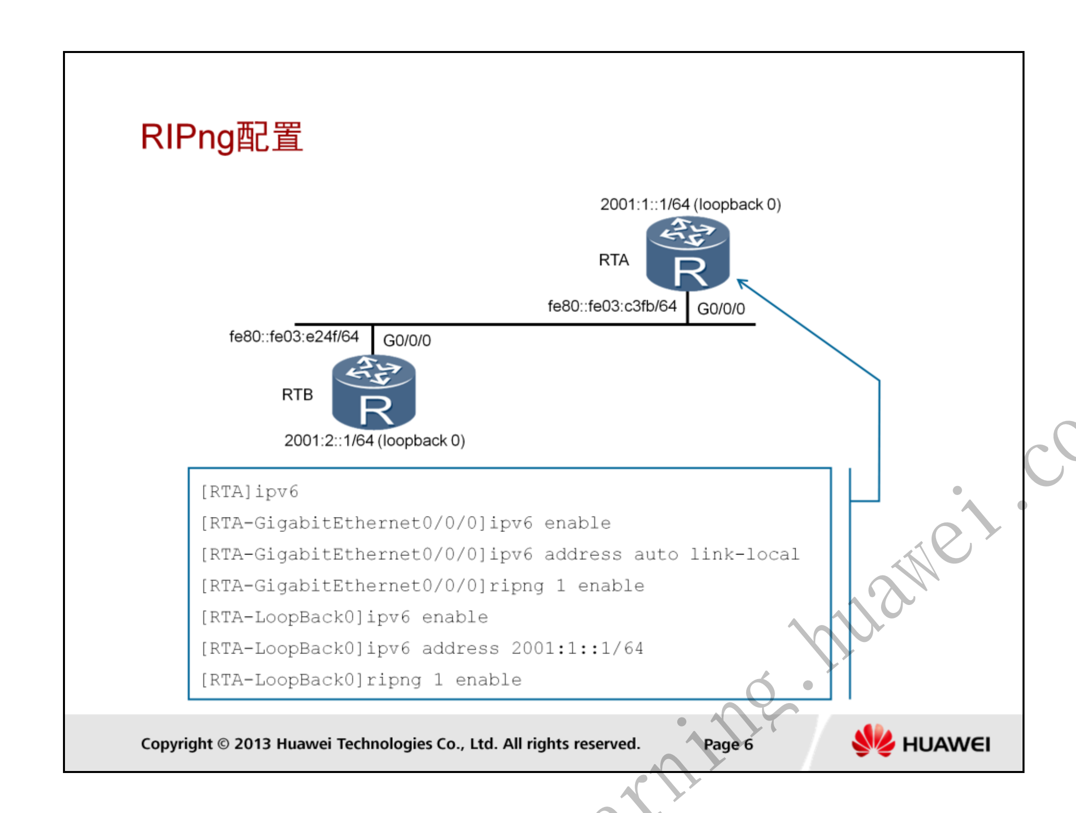


RIPng通过UDP的521端口发送和接收路由信息。所有路由信息更新报文（包括定期发送报文和主动发送报文）都是在发送方和接收方的RIPng端口之间传输。有些请求报文可能来自RIPng端口以外的其它端口，但是报文会被转发到目标设备上的RIPng端口。

RIPng报头的Command字段定义报文的两种类型：一种是请求报文；另一种是响应报文。

Version字段指的是RIPng的版本。

每个RIPng报文可以包含一个或多个路由表项（RTE），每个路由表项中包含目的网络前缀、路由标记、前缀长度和度量值。



ipv6 enable命令用来在路由器接口上使能IPv6，使得接口能够接收和转发IPv6报文。接口的IPv6功能默认是去使能的。

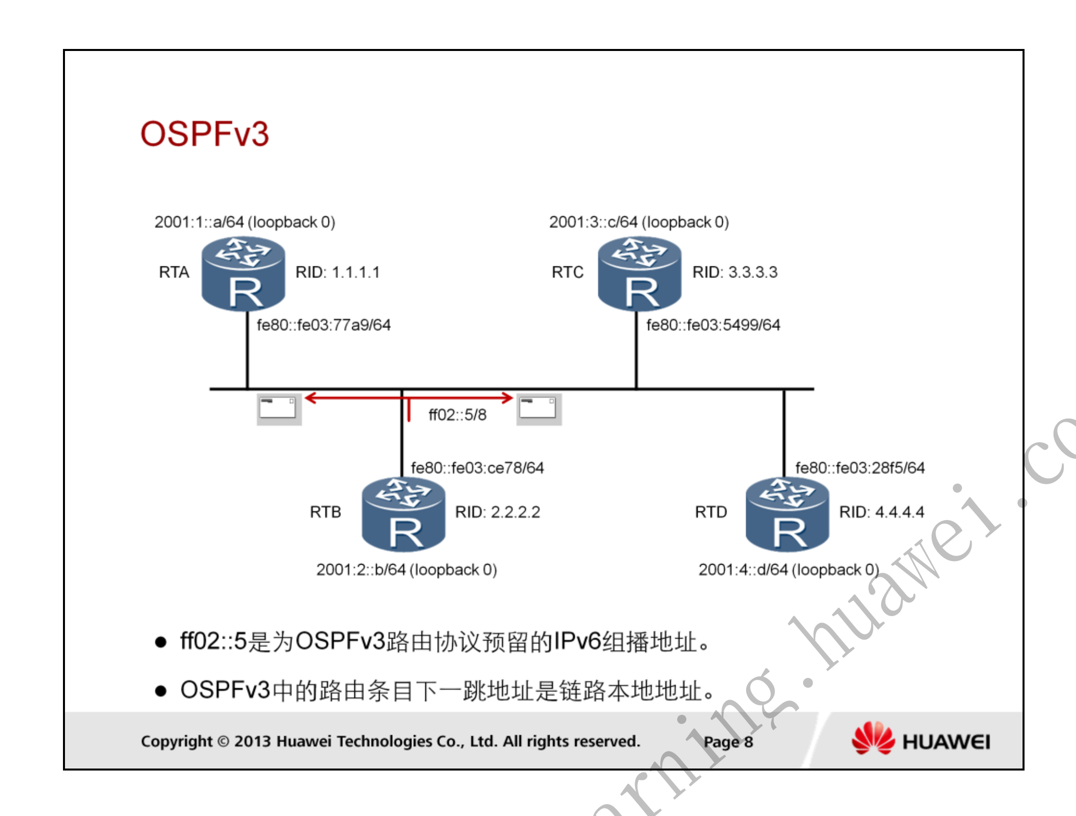
ipv6 address auto link-local命令用来为接口配置自动生成的链路本地地址。

ripng *process-id* **enable**命令用来使能一个接口的RIPng路由协议。进程ID可以是1到65535之间的任意值。缺省情况下，接口上未使能RIPng路由协议。

配置验证

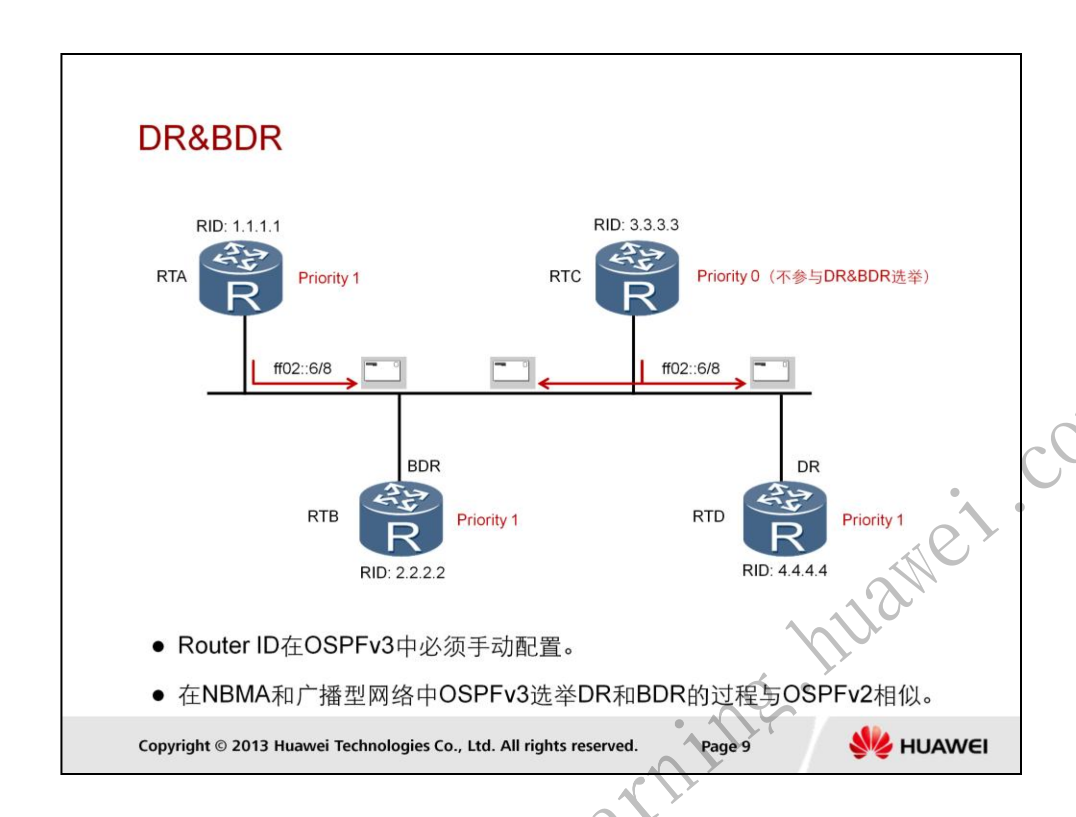
```
[RTA]display ripng
Public vpn-instance
    RIPng process : 1
       Preference     : 100              Checkzero      : Enabled
       Default-cost   : 0
       Maximum number of balanced paths : 8
       Update time    : 30 sec      Age time    : 180 sec
       Garbage-collect time : 120 sec
       Number of periodic updates sent : 217
       Number of trigger updates sent  : 1
       Number of routes in database    : 1
       Number of interfaces enabled    : 2
       Total number of routes : 0
       Total number of routes in ADV DB is : 1
  ......
```


执行**display ripng**命令，可以查看RIPng进程实例以及该实例的相关参数和统计信息。从显示信息中可以看出，RIPng的协议优先级是100，路由信息的更新周期是30秒。Number of routes in database字段显示为1，表明RIPng数据库中路由的条数为1。Total number of routes in ADV DB is字段显示为1，表明RIPng正常工作并发送了1条路由更新信息。



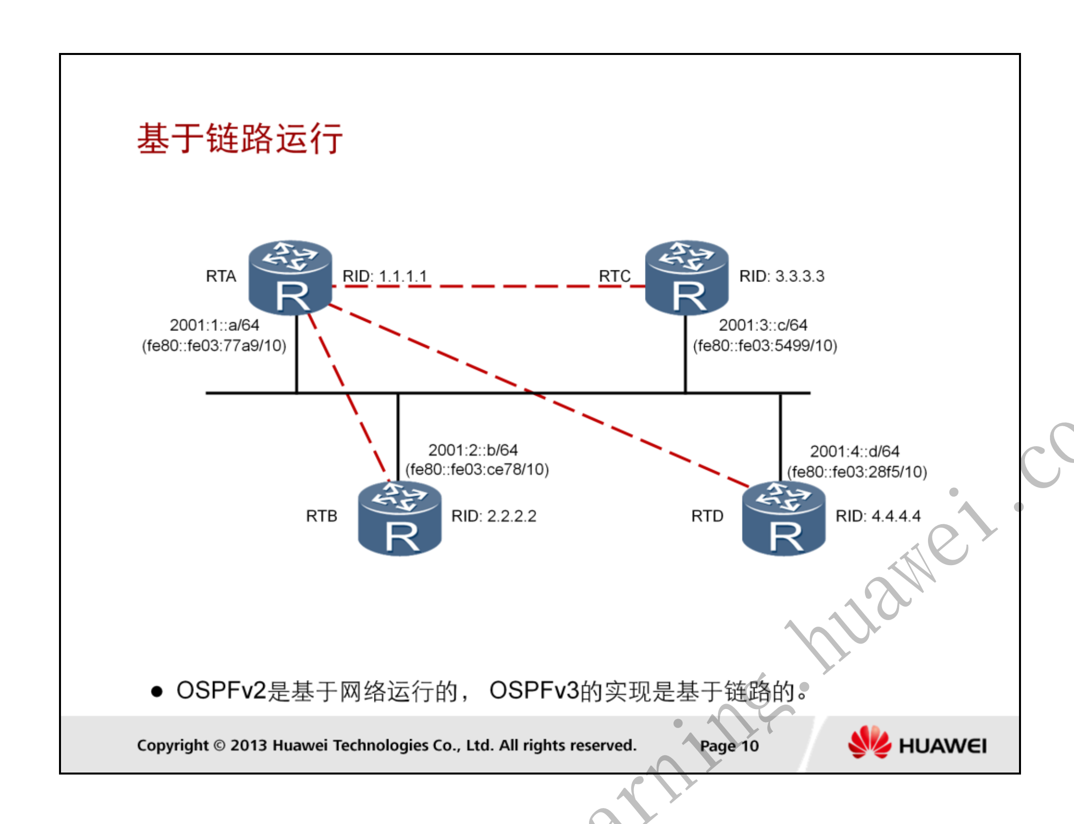
OSPFv3是运行在IPv6网络的OSPF协议。运行OSPFv3的路由器使用物理接口的链路本地单播地址为源地址来发送OSPF报文。相同链路上的路由器互相学习与之相连的其它路由器的链路本地地址，并在报文转发的过程中将这些地址当成下一跳信息使用，虚链路的场景不在本课程的讨论范围内。

IPv6中使用组播地址ff02::5来表示AllSPFRouters，而OSPFv2中使用的是组播地址224.0.0.5。需要注意的是，OSPFv3和OSPFv2版本互不兼容。

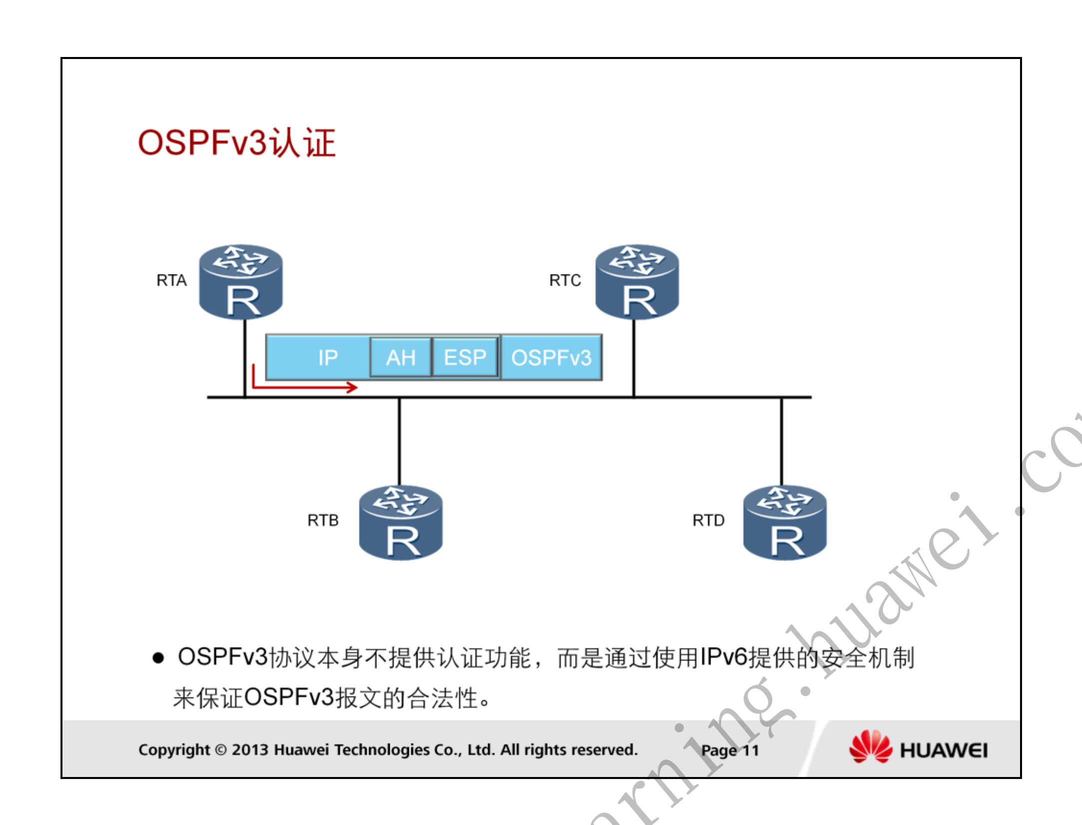


Router ID在OSPFv3中也是用于标识路由器的。与OSPFv2的Router ID不同，OSPFv3的Router ID必须手工配置；如果没有手工配置Router ID，OSPFv3将无法正常运行。OSPFv3在广播型网络和NBMA网络中选举DR和BDR的过程与OSPFv2相似。

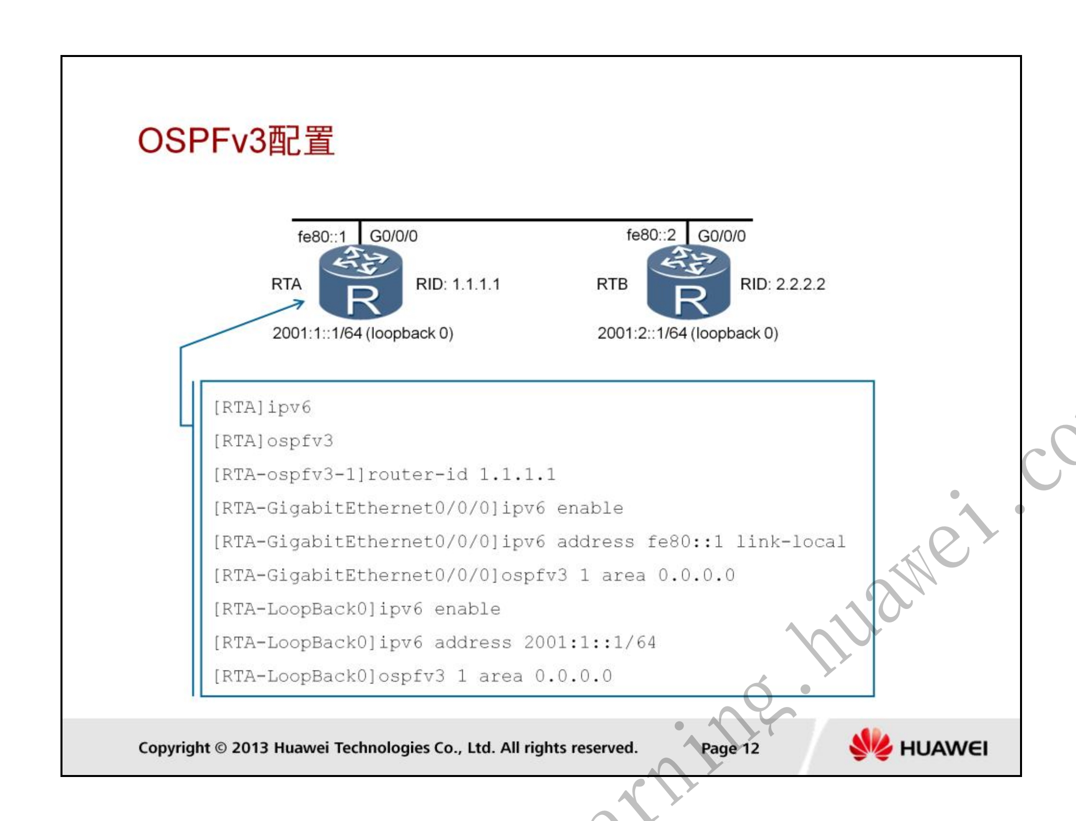
IPv6使用组播地址FF02::6表示AllDRouters，而OSPFv2中使用的是组播地址224.0.0.6。



OSPFv3是基于链路而不是网段的。在配置OSPFv3时，不需要考虑路由器的接口是否配置在同一网段，只要路由器的接口连接在同一链路上，就可以不配置IPv6全局地址而直接建立联系。这一变化影响了OSPFv3协议报文的接收、Hello报文的内容以及网络LSA的内容。



OSPFv3直接使用IPv6的扩展头部（AH和ESP）来实现认证及安全处理，不再需要OSPFv3自身来完成认证。



ipv6命令用来使能路由器的IPv6功能。要在路由器上运行OSPFv3协议，首先必须使能IPv6功能。

ospfv3 [*process-id*]命令用来创建并运行OSPFv3进程，*process-id*取值范围是1～65535。如果不指定进程号，缺省使用进程号1。

router-id *router-id*命令用来设置运行OSPFv3协议的路由器ID号。

ipv6 enable命令用来在路由器接口上使能IPv6，使得接口能够接收和转发IPv6报文。接口的IPv6功能默认是去使能的。**ipv6** *<link local address>* **link-local**命令用来手动为接口配置链路本地地址。

ospfv3 *process-id* **area** *area-id*命令用来在接口上使能OSPFv3的进程，并指定所属区域。

本示例中，路由器RTA的loopback接口和GigabitEthernet0/0/0接口都启用OSPFv3进程，并且都属于区域0。

配置验证

```
[RTA]display ospfv3
 Routing Process "OSPFv3 (1)" with ID 1.1.1.1
 Route Tag: 0
 Multi-VPN-Instance is not enabled
 SPF Intelligent Timer[millisecs] Max: 10000, Start: 500, Hold: 2000
 LSA Intelligent Timer[millisecs] Max: 5000, Start: 500, Hold: 1000
 LSA Arrival interval 1000 millisecs
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 Number of AS-External LSA 0. AS-External LSA's Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0. AS-Scoped Unknown LSA's Checksum
Sum 0x0000
 Number of FULL neighbors 1
 Number of Exchange and Loading neighbors 0
......
```




在邻居路由器上完成OSPFv3配置后，执行**display ospfv3**命令可以验证OSPFv3配置及相关参数。从显示信息中可以看到正在运行的OSPFv3进程为1，Router ID为1.1.1.1，Number of FULL neighbors值为1。



1. RIPng通过UDP端口号521接收其它路由器发送的路由更新。
2. Router ID用于唯一标识一台运行OSPFv3协议的路由器。


谢谢
www.huawei.com


DHCPv6原理与配置
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI



前言

主机在运行IPv6时，可以通过使用无状态地址自动配置或DHCPv6协议来获取IPv6地址。IPv6动态主机配置协议DHCPv6(Dynamic Host Configuration Protocol for IPv6)采用了客户端/服务器通信模式，是针对IPv6编址方案设计的、为主机分配IPv6地址和其他网络配置参数的协议。

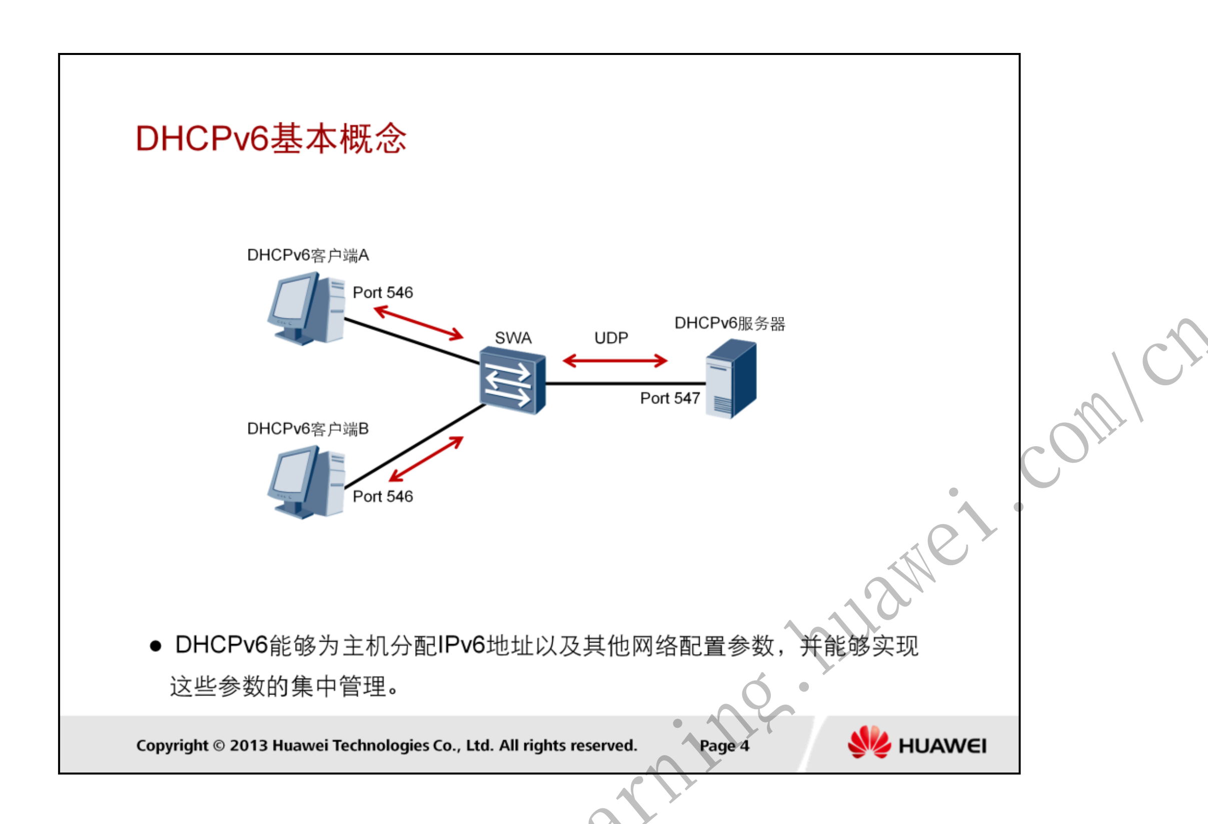




学习目标

学完本课程后，您应该能：

- 掌握DHCPv6的工作原理
- 掌握DHCPv6的配置

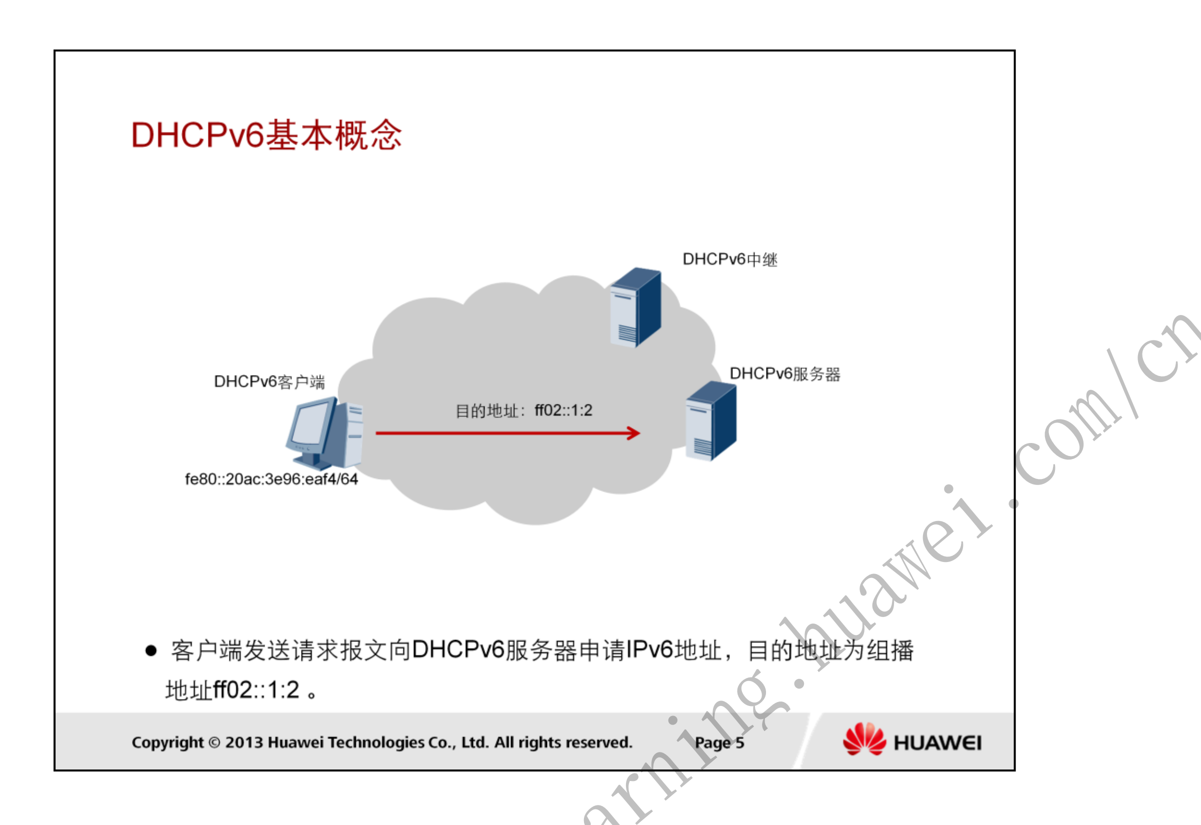


主机在运行IPv6时，可以通过使用无状态地址自动配置或DHCPv6协议来获取IPv6地址。

主机使用无状态地址自动配置方案来获取IPv6地址时，路由器并不记录主机的IPv6地址信息，可管理性差；另外，IPv6主机无法获取DNS服务器地址等网络配置信息，在可用性上也存在一定的缺陷。

DHCPv6属于一种有状态地址自动配置协议。在有状态地址配置过程中，DHCPv6服务器为主机分配一个完整的IPv6地址，并提供DNS服务器地址等其他配置信息。此外，DHCPv6服务器还可以对已经分配的IPv6地址和客户端进行集中管理。

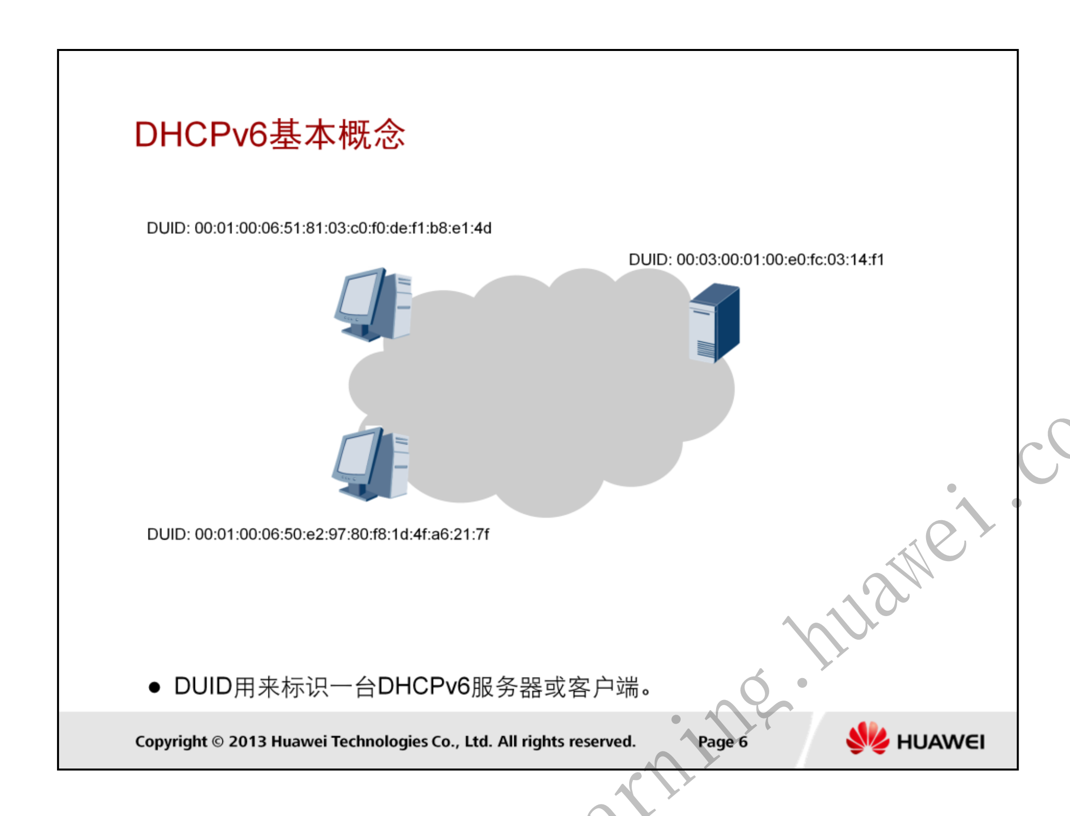
DHCPv6服务器与客户端之间使用UDP协议来交互DHCPv6报文，客户端使用的UDP端口号是546，服务器使用的UDP端口号是547。



DHCPv6基本协议架构中，主要包括以下三种角色：

1. DHCPv6客户端：通过与DHCPv6服务器进行交互，获取IPv6地址/前缀和网络配置信息，完成自身的地址配置功能。
2. DHCPv6中继：负责转发来自客户端方向或服务器方向的DHCPv6报文，协助DHCPv6客户端和DHCPv6服务器完成地址配置功能。只有当DHCPv6客户端和DHCPv6服务器不在同一链路范围内，或者DHCPv6客户端和DHCPv6服务器无法单播交互的情况下，才需要DHCPv6中继的参与。
3. DHCPv6服务器：负责处理来自客户端或中继的地址分配、地址续租、地址释放等请求，为客户端分配IPv6地址/前缀和其他网络配置信息。

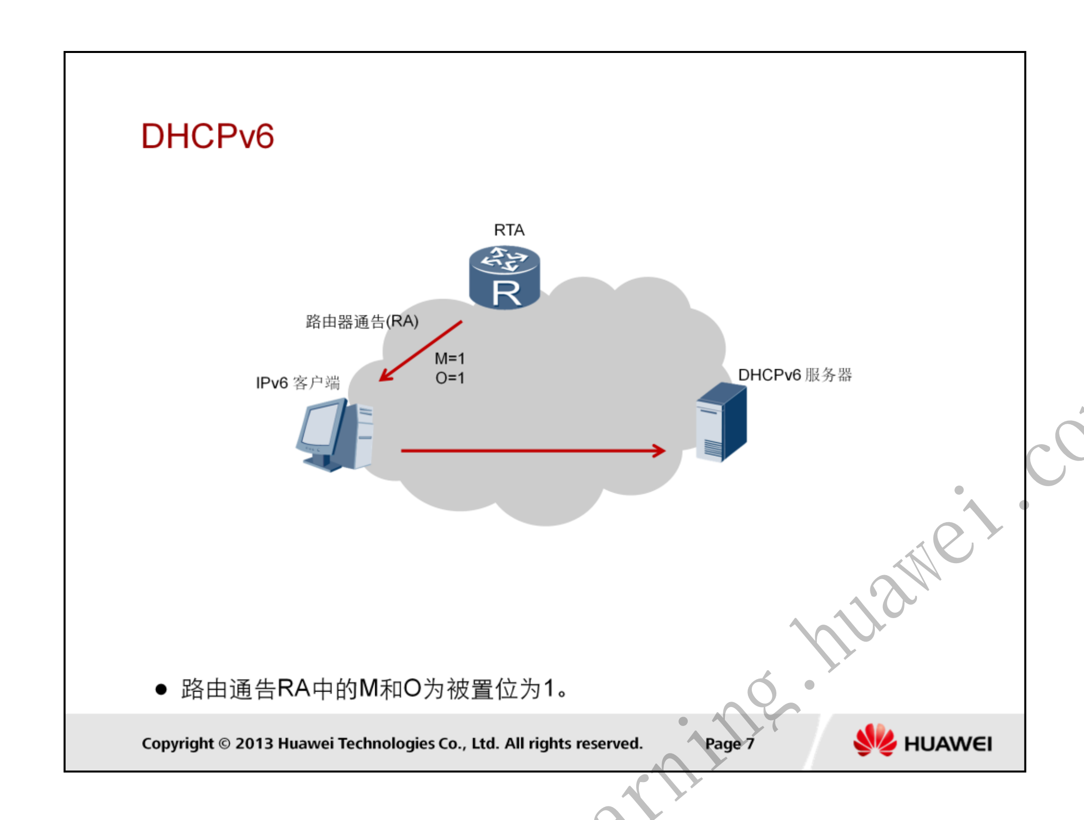
客户端发送DHCPv6请求报文来获取IPv6地址等网络配置参数，使用的源地址为客户端接口的链路本地地址，目的地址为ff02::1:2。ff02::1:2表示的是所有DHCPv6服务器和中继，这个地址是链路范围的。



DHCP设备唯一标识符DUID（DHCPv6 Unique Identifier）用来标识一台DHCPv6服务器或客户端。每个DHCPv6服务器或客户端有且只有一个DUID。

DUID采用以下两种方式生成：

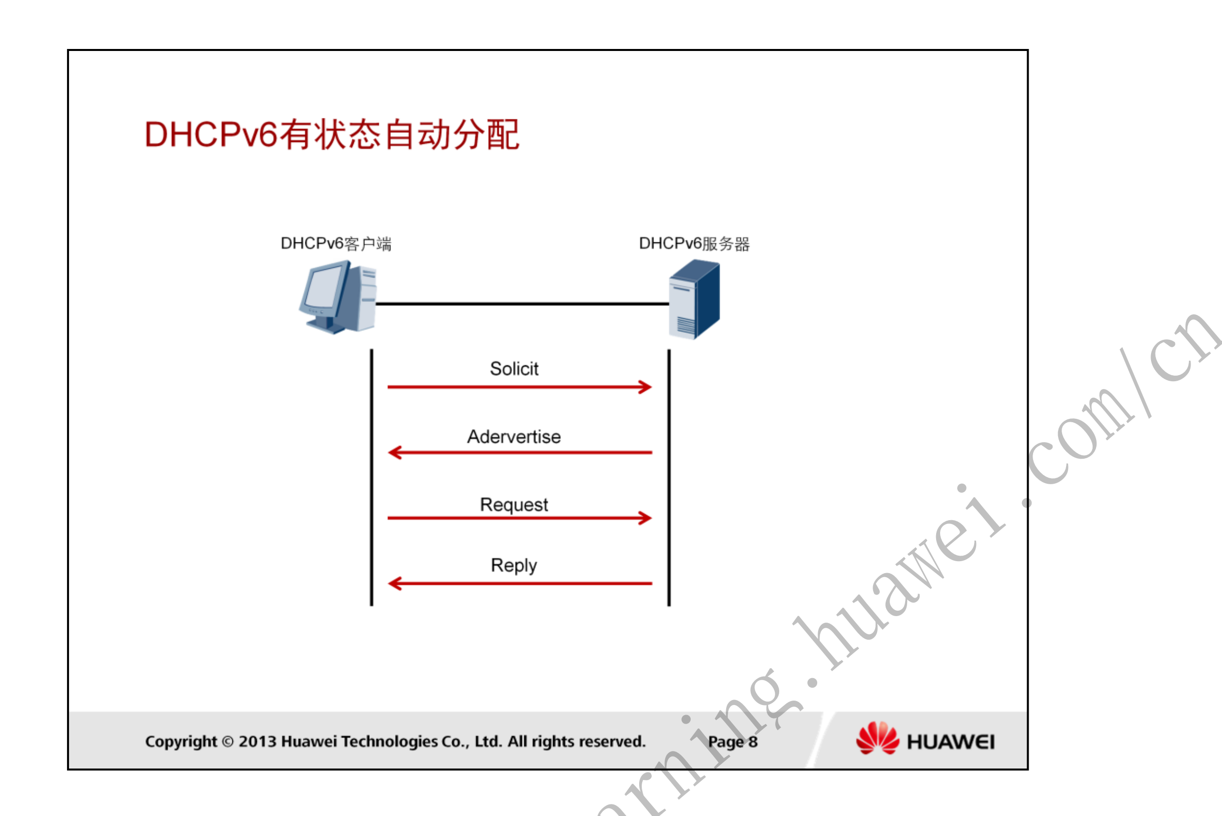
1. 基于链路层地址（LL）：即采用链路层地址方式来生成DUID。
2. 基于链路层地址与时间组合（LLT）：即采用链路层地址和时间组合方式来生成DUID。



DHCPv6分配地址时又分为:

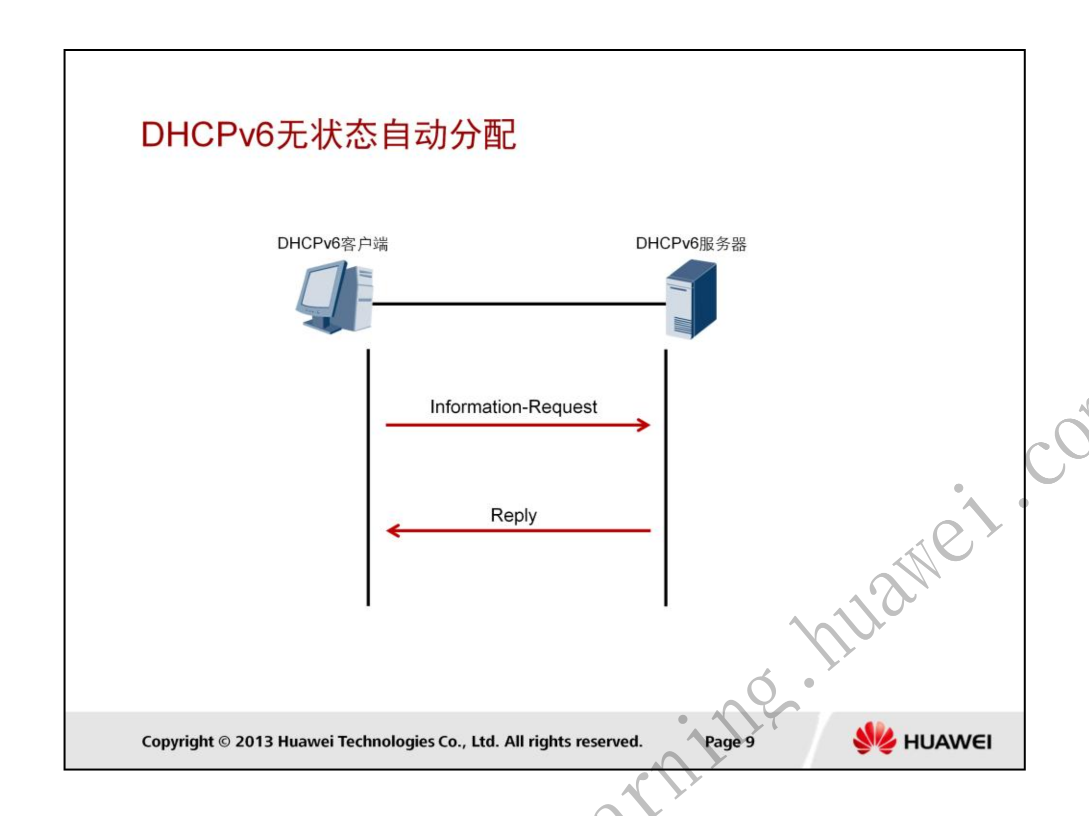
1. DHCPv6有状态自动分配：DHCPv6服务器为客户端分配IPv6地址及其他网络配置参数（如DNS、NIS、SNTP服务器地址等）。
2. DHCPv6无状态自动分配：主机的IPv6地址仍然通过路由通告方式自动生成，DHCPv6服务器只分配除IPv6地址以外的配置参数（如DNS、NIS、SNTP服务器等）。

DHCPv6客户端在向DHCPv6服务器发送请求报文之前，会发送RS报文，在同一链路范围的路由器接收到此报文后会回复RA报文。在RA报文中包含管理地址配置标记（M）和有状态配置标记（O）。当M取值为1时，启用DHCPv6有状态地址配置，即DHCPv6客户端需要从DHCPv6服务器获取IPv6地址，取值为0则启用IPv6无状态地址自动分配方案。当O取值为1时，用来定义客户端需要通过有状态的DHCPv6来获取其它网络配置参数，如DNS、NIS、SNTP服务器地址等，取值为0则启用IPv6无状态地址自动分配方案。



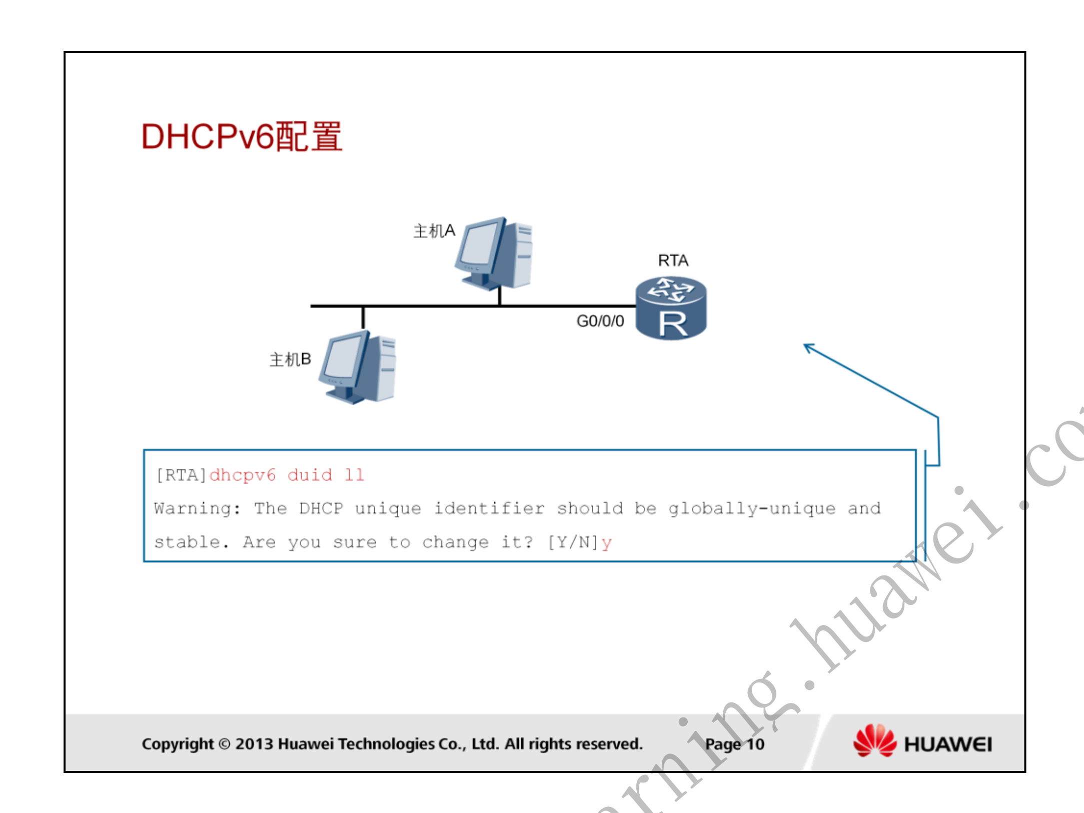
DHCPv6四步交互地址分配过程如下:

1. DHCPv6客户端发送Solicit报文，请求DHCPv6服务器为其分配IPv6地址和网络配置参数。
2. DHCPv6服务器回复Advertise报文，该报文中携带了为客户端分配的IPv6地址以及其它网络配置参数。
3. DHCPv6客户端如果接收到了多个服务器回复的Advertise报文，则会根据Advertise报文中的服务器优先级等参数来选择优先级最高的一台服务器，并向所有的服务器发送Request组播报文。
4. 被选定的DHCPv6服务器回复Reply报文，确认将IPv6地址和网络配置参数分配给客户端使用。



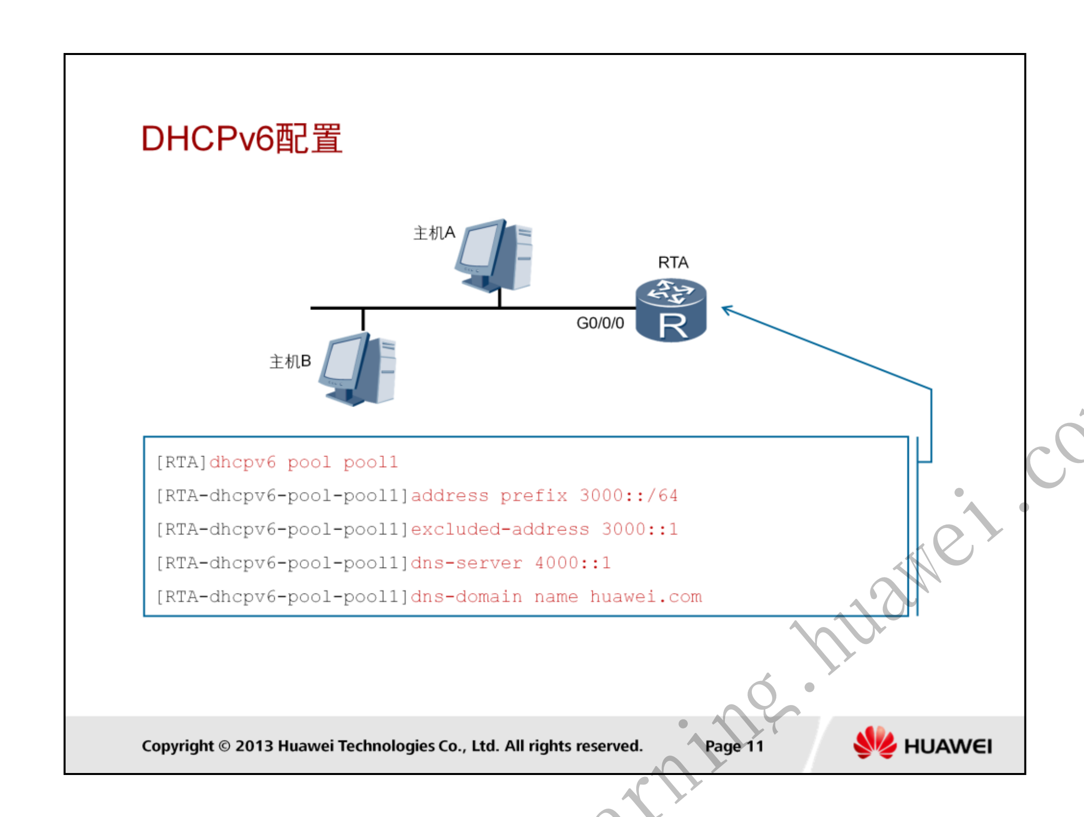
DHCPv6无状态工作过程如下:

1. DHCPv6客户端以组播方式向DHCPv6服务器发送Information-Request报文，该报文中携带Option Request选项，用来指定DHCPv6客户端需要从DHCPv6服务器获取的配置参数。
2. DHCPv6服务器收到Information-Request报文后，为DHCPv6客户端分配网络配置参数，并单播发送Reply报文，将网络配置参数返回给DHCPv6客户端。
3. DHCPv6客户端根据收到的Reply报文中提供的参数完成DHCPv6客户端无状态配置。



dhcpv6 duid { **ll** | **llt** }命令可以用来指定DUID格式为DUID-LL或DUID-LLT。缺省情况下，ARG3系列路由器采用的DUID格式是DUID-LL。当使用DUID-LLT格式时，时间戳值引用的是从执行**dhcpv6 duid llt**命令的时间点开始计算的时间。

可以使用**display dhcpv6 duid**命令来验证当前使用的DUID格式以及DUID值。

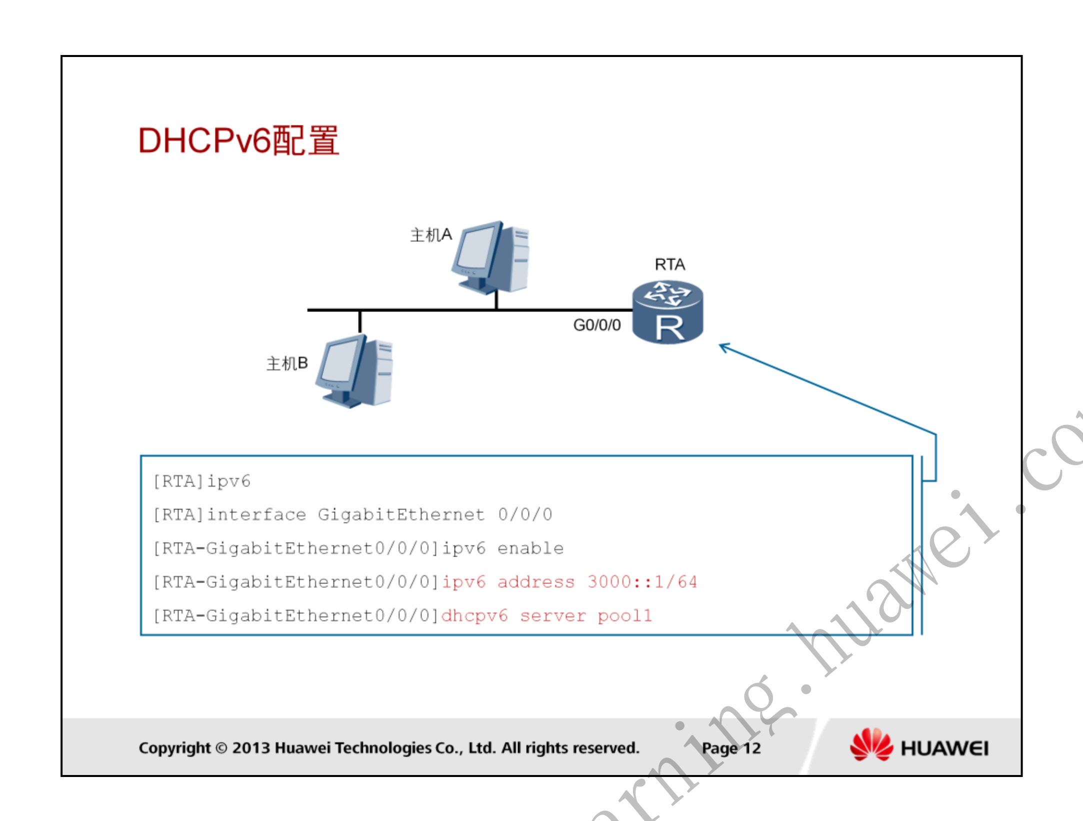


dhcpv6 pool *pool-name*命令用来创建IPv6地址池或进入到IPv6地址池视图。

address prefix *ipv6-prefix/ipv6-prefix-length*命令用来在IPv6地址池视图下绑定IPv6地址前缀。*ipv6-prefix/ipv6-prefix-length*用来指定IPv6地址池绑定的网络前缀和前缀长度。

excluded-address *start-ipv6-address* [**to** *end-ipv6-address*]命令用来配置IPv6地址池中不参与自动分配的IPv6地址范围。

dns-server *ipv6-address*命令用来配置DNS服务器的IPv6地址。**dns-domain-name** *dns-domain-name*命令用来配置为DHCPv6客户端分配的域名后缀。



dhcpv6 server *pool-name*命令用来在接口下配置DHCPv6服务器功能，*pool-name*用来指定接口下配置的DHCPv6地址池名称。

配置验证

```
[RTA]display dhcpv6 pool
DHCPv6 pool: 1
  Address prefix: 3000::1/64
    Lifetime valid 172800 seconds, preferred 86400 seconds
    0 in use, 0 conflicts
  Information refresh time: 86400
  Conflict-address expire-time: 172800
  Active normal clients: 0
```




display dhcpv6 pool命令用来查看DHCPv6服务器上配置的地址池信息。

本例中，RTA上有一个DHCPv6地址池，该地址池关联的地址前缀为3000::1/64，生存周期为172800秒，即两天（缺省情况下，生存周期是86,400秒或1天）。在必要的情况下，可以在IPv6地址池视图下使用**information-refresh**命令重新配置其它配置信息。对于处在活跃状态的客户端从DHCPv6服务器租用的IPv6地址，可以查看相关的信息统计。



总结

- ARG3系列路由器生成DUID的方式有哪些?
- 如果主机收到的路由器通告信息中M和O 位被置1,主机将如何操作?



1. ARG3系列路由器支持DUID-LL和DUID-LLT格式生成DUID。
2. 当接收到携带M和O（比特值均为1）的RA报文时，主机将主动发现DHCPv6服务器用于有状态地址配置。配置信息包括IPv6地址和其它配置参数，例如地址前缀和DNS服务器地址等。


谢谢
www.huawei.com

华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- 1、华为E-learning 课程学习
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的“华为账号”和注册账号的“email地址”到 *Learning@huawei.com 申请权限。*
- 2、华为培训教材下载
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训->面授培训*”，在具体课程页面即可下载教材。
- 3、华为在线公开课(LVC)优先参与
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- 4、学习工具 eNSP
  - *eNSP (Enterprise Network Simulation Platform)*, 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html）

